DEMANDE DE RENSEIGNEMENTS AU SUJET D'UN SYSTÈME DE GESTION DES DEMANDES DE SERVICES LINGUISTIQUES (SGDSL) POUR EMPLOI ET DÉVELOPPEMENT SOCIAL CANADA

Demande de renseignements (DR) No. : 100026030

Publiee le : 2024-03-14

Date limite pour les questions : 2024-04-05

Date limite pour les addendas (reponses fournies) : 2024-04-10

Date limite de soumission : 2024-04-13

adressez les demandes a la personne-resource de la DR : David Priori (nc-solicitations-gd@hrsdc-rhdcc.gc.ca)

TABLE DES MATIÈRES

DEMANDE DE RENSEIGNEMENTS AU SUJET D'UN SYSTÈME DE GESTION DES DEMANDES DE SERVICES LINGUISTIQUES (SGDSL) POUR EMPLOI ET DÉVELOPPEMENT SOCIAL CANADA

1.0 Contexte

Emploi et Développement social Canada (EDSC) sollicite les avis de l'industrie sur une solution de Système de gestion des demandes de services linguistiques (SGDSL) sur le Web, afin de remplacer sa solution actuelle.

Depuis de nombreuses années, EDSC utilisait Multi-Trans Prism comme solution sécurisée et complète de gestion des demandes de services linguistiques. Cette solution permettait d'exécuter et de gérer les services, les processus et les activités de traduction et d'interprétation de bout en bout d'EDSC, d'une manière intégrée à un niveau de sécurité Protégé B s'appliquant aux renseignements, aux biens et aux renseignements d'affaires.

Malheureusement, la solution SGDSL actuelle n'est plus prise en charge par son fournisseur et EDSC doit la remplacer pour répondre à ses besoins linguistiques dans l'ensemble du ministère. L'urgence est de remplacer MultiTrans Prism, le logiciel de mémoire de traduction. Il est important de connaître toutes les fonctionnalités actuellement disponibles pour les logiciels de mémoire de traduction. En outre, l'EDSC souhaite connaître les fonctionnalités actuellement disponibles pour les plateformes de gestion des demandes de Solutions SGDSL, les outils de gestion de la charge de travail et du flux de travail ainsi que les outils pouvant être inclus dans les solutions SGDSL qui combinent la mémoire de traduction et la traduction pilotée par l'IA et qui pourraient être accessibles au personnel non linguistique. L'outil devrait d'abord puiser dans la mémoire de traduction, à des fins de cohérence et de qualité, et une fois qu'il aurait tiré tout ce qu'il pouvait des mémoires de traduction, les parties non traduites du texte seraient traduites au moyen de la traduction neuronale (IA)

2.0 Objet de la DR

Cette DR a pour objectif de :

a. Identifier l'état actuel des fonctionnalités et de la technologie disponibles pour une solution de système de gestion des demandes de services linguistiques et en particulier pour le logiciel de mémoire de traduction;
b. Déterminer s'il existe des logiciels commerciaux prêts à l'emploi (COTS) qui pourrait répondre à la majorité des exigences techniques et non techniques d'une solution;
c. Évaluer les coûts de développement et le temps nécessaires pour répondre à l'ensemble des besoins s'il n'existe pas de produit COTS répondant à la majorité des exigences; et
d. Affiner la planification et le budget des dépenses.

3.0 Composantes et services généraux de la solution SGDSL actuelle

<u>La solution SGDSL actuelle comprend</u> :

1. Le portail pour les ressources et les clients;
2. La gestion du flux de travail;
3. La gestion de la charge de travail;
4. La gestion de la terminologie;
5. Les outils de traduction assistée par ordinateur (TAO);
6. Les outils d'assurance qualité;
7. Les fonctions d'analyse, de rapport et d'audit;
8. L'interopérabilité de gestion financière;
9. La gestion de la sécurité;
10. L'évolutivité pendant la durée du contrat existant; et
11. La gestion des documents.

La solution actuelle se compose de deux éléments : Flow qui est hébergé sur les serveurs de l'entrepreneur et qui est utilisé pour créer des demandes de traduction; et le système qui gère le stockage de la base de texte/termbase qui est hébergé en interne à l'EDSC. Les traducteurs utilisent la composante interne pour leur travail. La composante hébergée sur les serveurs du fournisseur est et doit continuer à être entièrement hébergée au Canada, ce qui inclut les centres de données de l'entrepreneur ou du sous-traitant, l'infrastructure de service sous-jacente, le réseau, la base de données, le web, les serveurs d'application, les systèmes d'exploitation, les machines virtuelles et l'espace de stockage. À l'avenir, les attributs intéressants comprennent la fonctionnalité de recherche basée sur les champs à déclarer, les attributs des documents et les métadonnées.

La solution SGDSL est et devrait continuer :

- D'être un outil interactif et personnalisable sur le web qui peut être facilement configuré par les utilisateurs pour refléter leurs besoins spécifiques;
- De permettre la définition des rôles des utilisateurs, des droits d'accès et des autorisations pour la solution, la suite d'outils, les caractéristiques et les fonctionnalités;
- De disposer d'un flux de travail et de règles opérationnelles à configurer par l'utilisateur pour prendre en charge une grande variété de processus, d'activités et de fonctions;
- De permettre une gestion efficace des métadonnées et des données — par exemple, toutes les données seront saisies une seule fois et validées dans la solution, avec la possibilité de réutiliser et d'exploiter les données dans l'ensemble de la solution et de ses fonctionnalités;
- De permettre un partage direct sans interruption des données au sein de la solution et d'autres systèmes connexes hébergés par l'entrepreneur;
- De permettre la réutilisation des données communément requises de manière sécurisée dans l'ensemble de la solution et d'autres systèmes d'EDSC; et
- De permettre une variation constante et un accès en temps réel aux données, aux rapports et aux informations analytiques afin de soutenir la gestion efficace et la prise de décision opérationnelle, la surveillance et le suivi des processus et des performances.

Les composantes clés de la solution actuelle et future sont les suivantes :

a. **La mémoire de traduction** qui :

- Stocke les documents afin que les traducteurs/réviseurs/spécialistes linguistiques puissent construire une base de textes, y compris les traductions effectuées dans le passé ou à partir de sources externes à la solution,
- Comprend une base de données terminologique;
- Permet de mettre à jour le texte et les bases de données terminologiques (correction et manipulation du texte dans la mémoire elle-même, plutôt que de devoir retourner dans le fichier pour corriger une erreur et le télécharger à nouveau dans la mémoire de traduction);
- Est accessible en dehors du réseau (au cas où le RPV ne serait pas accessible pour une raison quelconque); et
- Comprend toutes les fonctionnalités de base d'une mémoire de traduction.

b. **La plateforme de gestion des demandes** qui :

- Permet de gérer les demandes, ainsi que les profils des clients et des prestataires (mise à jour, édition, suppression). Doit être accessible hors réseau.

c. **Gestion du flux et de la charge de travail** qui :

- Permet à un utilisateur ayant le rôle, les droits d'accès et les autorisations appropriés de configurer le flux de travail pour prendre en charge une variété de processus, d'activités et de fonctions.

d. **Outils pour le personnel non linguistique** qui :

- Combine la mémoire de traduction et la traduction pilotée par l'IA qui pourrait être accessible au personnel non linguistique (comme les développeurs). L'outil puiserait d'abord dans la mémoire de traduction, à des fins de cohérence et de qualité, et une fois qu'il aurait tiré tout ce qu'il pouvait des mémoires de traduction, les parties non traduites du texte seraient traduites au moyen de la traduction neuronale (IA) et stockées dans la mémoire de traduction (pour consultation et révision ultérieures).

4.0 Disponibilité, volume de transactions, données et confidentialité

Disponibilité :

La solution doit actuellement être accessible à l'utilisateur 24 heures sur 24 et 7 jours sur 7. Il devrait en être de même à l'avenir.

Nombre de transactions :

En ce qui concerne le volume des transactions en cours, on compte annuellement **des milliers de demandes de traduction (toutes équipes de services linguistiques confondues) et des centaines de milliers (au moins) de textes stockés en mémoire, sans compter les bases terminologiques**.

Données et renseignements :

Toutes les données et tous les renseignements qui sont migrés, archivés, sauvegardés, stockés sur des supports, créés ou associés à la solution SGDSL, actuellement et à l'avenir, sont et demeureront en tout temps la propriété du Canada et, à ce titre, doivent être cryptés conformément aux exigences de sécurité du gouvernement du Canada. Le format des données doit rester le même que celui d'origine et ne doit pas être converti dans un format propriétaire, car EDSC doit pouvoir accéder à ses données à tout moment.

À l'avenir, le CESD souhaiterait disposer d'une fonctionnalité permettant à un utilisateur ayant le rôle, les droits d'accès et l'autorisation appropriés d'adapter et de configurer l'interface et les attributs de l'utilisateur, de contrôler le comportement de l'entreprise (par exemple, les conditions qui doivent être remplies avant que l'utilisateur puisse modifier une demande de service) à l'aide de règles d'entreprise et de la validation des données d'entrée.

5.0 Accès au système et interface utilisateur

Accès sur le Web : Les caractéristiques et fonctionnalités de la solution SGDSL pour la traduction, la terminologie et l'interprétation sont actuellement et devront à l'avenir être basées sur le web et comprennent des portails (client, ressource(s) interne(s) et externe(s)), des tableaux de bord, un flux de travail, une charge de travail, une terminologie, une gestion de la sécurité, des outils de traduction assistée par ordinateur (TAO), des mémoires de traduction, une base de données terminologiques, des analyses, des rapports et une veille économique.

À l'avenir, le CESD souhaiterait pouvoir configurer l'interface utilisateur de la manière suivante :

a) Ajouter de nouveaux attributs ou modifier la fonctionnalité des attributs existants;
b) Définition des types d'attributs tels que les nombres, le texte libre, les listes de sélection et les booléens;
c) Définition de la position de l'interface graphique des attributs et de l'ordre des onglets;
d) Définition du comportement et des propriétés au niveau des attributs, tels que les étiquettes, curseur de souris sur le bouton « Aide », le caractère obligatoire/optionnel, la visibilité et la valeur par défaut;
e) Création de règles de gestion et validation des données d'entrée;
f) Réglage de la mise en page de l'impression;
g) Spécifier quels attributs de données sont préremplis lors de la création de l'artefact (par exemple, préremplir les données de l'utilisateur à partir du profil de l'utilisateur du demandeur sur une demande d'achat lors de la création d'une demande);
h) Spécifier le comportement à l'aide de règles de gestion, de règles de validation qui s'appliquent lorsque le processus de gestion est modifié;
i) Suivre et pouvoir afficher les changements (historique) pour chaque entrée et transaction commerciale;
j) Modification des informations, modification du déroulement des opérations d'approbation ou de rejet, modification des soumissions à des ressources externes, et confirmation;
k) Configurer la présentation de l'interface utilisateur d'un portail; et
l) Identifier et soumettre au contractant les modifications apportées aux valeurs de données codées en dur, des attributs et champs dans l'interface utilisateur.

L'interface du composant de la solution SGDSL fournit de brèves instructions et des conseils à l'utilisateur de manière cohérente pour toutes les commandes et tous les affichages. L'interface du composant de la solution SGDSL suit une norme, un thème et un ton de texte pour l'ensemble du composant. Il permet de personnaliser la sélection des couleurs et d'autres options de configuration visuelle pour permettre à l'EDSC de donner une image de marque à l'interface.

Disponibilité en anglais et en français :

L'ensemble de la solution SGDSL est actuellement disponible dans les deux **langues officielles** du Canada et comprend les éléments suivants : interface utilisateur web et application, système, outils, documentation, formation, service d'assistance. Les outils et applications de la solution SGDSL offrent à tous les utilisateurs la possibilité de définir une langue préférée par défaut pour leur utilisation, si l'utilisateur n'a pas indiqué de préférence. À l'avenir, les éléments de l'interface utilisateur de la solution devraient être disponibles dans les deux langues officielles du Canada et inclure :

a) Contrôles des données d'entrée : cases à cocher, boutons radio, listes déroulantes, boîtes à liste, boutons, bascules, champs de texte, champ de date, fenêtre de terminal de texte;
b) Composants de navigation : fil d'Ariane, curseur, champ de recherche, pagination, curseur, étiquettes, icônes, onglets;
c) Composants informationnels : infobulles, icônes, barre de progression, notifications, boîtes ou fenêtres de message, boîtes de dialogue, fenêtres modales (pop up);
d) Menus : barre de menu, menu, menu contextuel, menus supplémentaires, menus primaires et secondaires :
e) Navigateur : tels que Edge, Chrome et Firefox;
f) Page principale, page d'accueil, page de bienvenue ou de connexion — devrait être configurable, mais pour l'instant, les informations protégées B ne sont pas autorisées; et
g) Lorsqu'il utilise les outils et les applications de la solution SGDSL, l'utilisateur doit pouvoir basculer entre l'une ou l'autre des langues officielles du Canada.

Il est prévu qu'à l'avenir, les outils et applications de la solution SGDSL permettent de saisir certains champs de contrôle dans les deux langues officielles du Canada, quelle que soit la langue choisie par l'utilisateur. Il doit être capable d'intégrer les informations sur les deux langues officielles du Canada dans sa (ses) base(s) de données. Les rapports générés à partir de la solution SGDSL, par les utilisateurs et les ressources, doivent également être disponibles dans les deux langues officielles du Canada.

6.0 Description et nombre d'utilisateurs actuels

Quatre types d'utilisateurs accèdent actuellement à la solution :

a. Les administrateurs système de la solution, qui ont pour rôle d'attribuer des droits et des privilèges aux différents types d'utilisateurs;

b. Utilisateurs à part entière (**traducteurs/réviseurs/spécialistes linguistiques uniquement**) qui utilisent les mémoires de traduction, entretiennent et alimentent les bases. Il y a environ 100 à 150 utilisateurs de ce type qui utilisent le système simultanément et ils sont considérés comme les utilisateurs les plus importants pour toute solution future. Ce type d'utilisateur est censé être le nombre minimum de ce type d'utilisateur. Ce nombre devrait augmenter.

Les services utilisés par les traducteurs/spécialistes linguistiques sont les suivants :

Service	Description
Adaptation	Traduire un document et y apporter des modifications afin d'adapter le message à son public cible. Il s'agit également de proposer des traductions possibles pour des programmes, des initiatives, des projets, etc., ainsi que des traductions de transcriptions.
Services administratifs	Traitement d'une demande nécessitant un volume inhabituel de traitement administratif. Exemple : demande comportant de nombreux fichiers, traitement de fichiers complexes et/ou nécessitant un traitement supplémentaire (tels que les fichiers PDF et JPG), fusion de fichiers, recherche de documents déjà traduits.
Révision comparative	Comparer soigneusement une traduction avec le texte original et corriger le contenu et le style de la traduction.
Édition (unilingue)	Améliorer un texte original en corrigeant la grammaire ou le style ou en proposant des solutions pour faciliter la lecture et la compréhension du texte.
Édition légère	Révision d'un texte pour corriger les erreurs de base, ainsi que pour signaler les phrases illogiques ou peu claires et les incohérences.
Conseil linguistique	Fournir des conseils sur les problèmes de traduction et les questions et problèmes linguistiques (grammaire, style, ponctuation, terminologie, etc.) sans qu'un document ne soit nécessaire.
Traduction sur place	Fournir les services d'un professionnel de la langue qui peut travailler de manière exclusive et autonome pour un client ou un groupe de clients dans nos bureaux.
Examen du langage clair et simple	Retravailler et restructurer un texte pour le rendre facile à lire, à comprendre et à utiliser. Travailler en étroite collaboration avec l'auteur, le conseiller en communication ou l'expert en la matière.
Gestion de projets	Planification, organisation, direction, contrôle et suivi d'un projet linguistique ou de traduction complexe.
Relecture	Lire un texte, identifier les erreurs ou les coquilles et indiquer les modifications à apporter.
Services de terminologie	Développer des glossaires personnalisés (à l'usage de notre équipe, de nos clients et de notre branche), participer à des comités et projets terminologiques.
Traduction	Réécrire un texte dans une autre langue en tenant compte du ton, du style et de la terminologie utilisés par l'auteur.
Traduction de documents modifiés	Traduire les modifications apportées à un document déjà traduit.
Traducteur en attente	Fournir les services d'un professionnel de la langue qui peut être joint à court terme, à tout moment et pour une période déterminée afin d'effectuer le travail d'un client. Le traducteur peut exercer d'autres activités pendant cette période.
Aide à la rédaction	Rédiger un texte en collaboration avec un client et fournir des conseils linguistiques sur les problèmes de traduction et les questions linguistiques (grammaire, style, ponctuation, terminologie, etc.)

c. Les coordinateurs/gestionnaires de projets, les gestionnaires/administrateurs, les prestataires (internes et externes), les clients (personnes non linguistiques) qui accèdent généralement à la plateforme de gestion pour formuler les demandes qui sont envoyées aux traducteurs, grâce à l'utilisation de Multi Trans Flow et de Terminotix. Il y a environ 50 -100 utilisateurs de ce type.

d. Le personnel non linguistique qui a besoin d'une traduction ad hoc ou d'une traduction urgente que son équipe de services linguistiques n'est pas en mesure de traiter, pour une raison ou une autre. Ils ont besoin d'accéder à une combinaison de la mémoire de traduction et de la partie de la solution consacrée à la traduction pilotée par l'IA pour les travaux qui ne sont pas déjà traduits par la mémoire de traduction de la solution. Il y a environ 200 utilisateurs de ce type, mais en fonction des outils disponibles dans une nouvelle solution, ce type d'utilisateur pourrait augmenter de manière significative. En fonction des outils disponibles dans une nouvelle solution, le nombre de ce type d'utilisateurs peut augmenter de manière significative par rapport à la base actuelle.

7.0 Environnement technique d'EDSC

La solution SGDSL doit être accessible avec Microsoft Windows 10 et 11, Sharepoint et Office 365, ainsi qu'avec différents navigateurs tels que Edge, Chrome et Firefox. Toutes les informations financières pertinentes de la solution sont transférées entre la solution SGDSL et SIGMA (SAP), à l'aide d'une fonctionnalité d'importation et d'exportation de fichiers vers et depuis une plateforme sécurisée.

La solution SGDSL offre actuellement les fonctionnalités suivantes :

a) Importer des données, des fichiers, des rapports, des analyses, des résultats de requêtes dans la solution SGDSL dans différents formats, notamment : MS Word (doc, docx), MS Excel (xls, xlsx), txt, pdf, xml, tmx, tbx, xliff et csv; et
b) Exporter des données, des fichiers, des rapports, des analyses, des résultats de requêtes à partir de la solution SGDSL dans différents formats, notamment : MS Word (doc.docx), MS Excel (xls, xlsx), txt, pdf, xml, tmx, tbx, xliff et csv.

Il prend en charge le protocole de transfert de fichiers sécurisé.

La solution actuelle fournit un accès sécurisé pour les clients, les ressources internes et externes sur la base des normes de sécurité informatique du gouvernement du Canada et des profils de contrôle de sécurité.

La solution actuelle est conforme à :

a. L'actuelle directive du SCT sur la gestion des projets et des programmes : Directive sur la gestion de projets et programmes — Canada.ca;
b. Norme sur l'accessibilité des sites Web Norme sur l'accessibilité des sites Web — Canada.ca;
c. Règles pour l'accessibilité du contenu Web, version 2.2 niveau AA (WCAG 2.2 AA);
d. La politique du SCT en matière de protection de la confidentialité et les directives connexes sur la protection de la confidentialité;
e. Normes et lignes directrices en matière de technologies de l'information (GSTI) — 33 sur la gestion des risques liés à la sécurité de la technologie de l'information;

f. La sécurité de l'informatique en nuage du gouvernement du Canada (stratégie d'adoption de l'informatique en nuage du GC, garde-fous de l'informatique en nuage du GC, modèle d'assurance par paliers du GC, gestion des risques liés à la sécurité de l'informatique en nuage ITSM.50.062, contrôles de sécurité, limites de confiance, interfaces standard et protocoles de sécurité, techniques utilisées pour la gestion des jetons — authentification et autorisation, méthodes de chiffrement, journalisation de la sécurité); et
g. 4.8 Autorisation et évaluation de la sécurité infonuagique ITSP.50.105.

8.0 Demande de renseignements (DR)

Il ne s'agit pas d'une demande de soumissions. Cette DR ne donnera pas lieu à l'octroi d'un contrat ou d'un marché. Par conséquent, les fournisseurs potentiels des biens ou des services décrits dans cette DR ne devraient pas réserver de stock ni d'installations, ni dégager des ressources en conséquence de tout renseignement contenu dans cette DR. Cette DR ne donnera pas lieu non plus à la création d'une liste de sources. Par conséquent, la réponse d'un fournisseur potentiel à cette DR n'empêchera pas ce fournisseur de participer à tout achat futur. De plus, l'achat de tout bien et service décrit dans cette DR ne suivra pas nécessairement cette DR. Cette DR vise simplement à solliciter les avis de l'industrie relativement aux questions décrites dans cette DR.

8.1 Nature et format des réponses demandées

Les fournisseurs qui répondent doivent fournir leurs commentaires, leurs préoccupations et, s'il y a lieu, leurs recommandations de rechange en ce qui a trait à la manière de répondre aux exigences ou aux objectifs décrits dans cette DR. Les fournisseurs sont aussi invités à fournir leurs commentaires au sujet du contenu, du format ou de l'organisation des ébauches de documents comprises dans cette DR. Les répondants devraient expliquer toutes les hypothèses qu'ils émettent dans leurs réponses.

8.2 Coûts de la réponse

Le Canada ne remboursera aucun répondant pour les dépenses encourues afin de répondre à cette DR.

8.3 Traitement des réponses

Utilisation des réponses : Les réponses ne feront pas l'objet d'une évaluation formelle. Cependant, les réponses pourraient être utilisées par le Canada pour élaborer ou modifier des stratégies d'approvisionnement ou toute ébauche de documents comprise dans cette DR. EDSC examinera toutes les réponses reçues avant la date limite de réception des DR. EDSC pourrait, à sa discrétion, examiner les réponses reçues après la date limite de réception des DR.

Équipe d'examen : Une équipe d'examen composée de représentants d'EDSC examinera les réponses. EDSC se réserve le droit d'embaucher tout consultant indépendant ou d'utiliser toute ressource du gouvernement qu'il juge nécessaire pour examiner toute réponse. Les membres de l'équipe d'examen n'examineront pas nécessairement l'ensemble des réponses.

Confidentialité : Les fournisseurs qui répondent doivent indiquer toutes les parties de leur réponse qu'ils jugent de nature exclusive ou confidentielle. EDSC traitera les réponses conformément à la *Loi sur l'accès à l'information*.

Les fournisseurs sont informés que toute information soumise à EDSC en réponse à la présente demande de renseignements peut être utilisée par EDSC pour finaliser un appel d'offres concurrentiel.

Toutes les consultations de l'industrie seront documentées et cette information est assujettie à la *Loi sur l'accès à l'information.* Les fournisseurs doivent indiquer toute information soumise qui doit être considérée comme confidentielle ou exclusive à l'entreprise. EDSC s'engage à ne pas divulguer au public ou à des tiers les informations désignées comme confidentielles ou exclusives.

Activité de suivi : EDSC peut rencontrer les Répondants qui répondent à la DR et indiquent dans leurs réponses qu'ils souhaitent participer à une réunion virtuelle de suivi. Lors de cette réunion, il sera demandé à chaque soumissionnaire à la DDR de démontrer la fonctionnalité de sa solution et en particulier d'identifier comment les traducteurs/réviseurs/spécialistes linguistiques accèderont à la solution et l'utiliseront. La date et l'heure de la réunion virtuelle de suivi seront communiquées aux fournisseurs au moins 10 jours ouvrables avant la réunion, qui devrait se tenir pendant les heures de travail normales et ne pas durer plus de 90 minutes.

Fourniture de documents justificatifs

Tout autre document qu'un fournisseur estime susceptible de fournir des informations pertinentes sur la solution proposée, la suite d'outils ou les applications tierces d'appui est le bienvenu.

8.4 Contenu de la présente DR

La présente demande de renseignements contient des questions spécifiques adressées aux représentants de l'industrie et fournit un formulaire de réponse à remplir par les représentants.

8.5 Format des réponses

a) **Page couverture** : Si la réponse comprend de multiples volumes, les fournisseurs doivent indiquer sur la première page couverture de chaque volume le titre de la réponse, le numéro de la demande, le numéro du volume et le nom légal complet du fournisseur.

Page de titre : La première page de chaque volume de la réponse, après la page couverture, devrait être la page de titre et elle devrait comprendre ce qui suit :

le titre de la réponse du fournisseur et le numéro du volume;
le nom et l'adresse du fournisseur;
le nom, l'adresse et le numéro de téléphone de la personne-ressource du fournisseur;
la date; et
le numéro de la DR.

Système de numérotation : Les fournisseurs qui répondent sont priés de préparer leur réponse en utilisant un système de numérotation correspondant à celui de la présente DR. Toutes

les références au matériel descriptif, aux manuels et aux brochures techniques inclus dans le cadre de la réponse devraient être faites en conséquence.

8.6 Demandes de renseignements

Puisqu'il ne s'agit pas d'une demande de soumissions, EDSC ne répondra pas nécessairement aux demandes de renseignements par écrit ou en transmettant les réponses à tous les fournisseurs éventuels. Cependant, les répondants qui ont des questions au sujet de cette DR peuvent transmettre leurs demandes de renseignements à :

Autorité contractante : David Priori
Courriel : NC-SOLICITATIONS-GD@hrsdc-rhdcc.gc.ca

8.7 Proposition des réponses

a) **Heure et lieu pour proposer les réponses** : Les fournisseurs désireux de fournir une réponse doivent l'envoyer par courriel à l'autorité contractante susmentionnée avant l'heure et la date indiquées sur la page de couverture du présent document.
b) **Responsabilité du respect des délais de livraison :** Il incombe à chaque fournisseur qui répond de s'assurer que sa réponse est envoyée à temps au bon endroit.

Annexe A Questions pour l'industrie

A1. Questions générales

Question	Informations sur le fournisseur
1. Décrivez brièvement votre entreprise, le lieu de son siège social, le nombre de personnes qu'elle emploie, depuis combien de temps elle est en activité, et indiquez le nombre d'installations et de sites (y compris les bureaux, les installations de stockage de données, l'emplacement des serveurs en nuage, etc.	
2. Identifiez les types de produits et de services linguistiques que vous fournissez (par exemple, etc.), depuis combien de temps ces solutions sont fournies, ainsi que le client type et le nombre d'utilisateurs pour chaque type de solution.	
3. Indiquez le nom et l'historique de la Solution proposée et donnez un aperçu de la fonctionnalité de la Solution de système de gestion des demandes de services linguistiques (SGDSL) que vous proposeriez à EDSC comme solution de remplacement. Indiquez si la solution proposée a été fournie à des clients du secteur public canadien, quand et depuis combien de temps.	
4. Identifiez, pour la solution que vous proposez, les fonctionnalités suivantes qui sont incluses sans développement supplémentaire et donnez des détails sur les fonctionnalités spécifiques : a. Le portail pour les ressources et les clients; b. La gestion du flux de travail; c. La gestion de la charge de travail; d. La gestion de la terminologie; e. Les outils de traduction assistée par ordinateur (TAO); f. Les outils d'assurance qualité; g. Les fonctions d'analyse, de rapport et d'audit;	

Question	Informations sur le fournisseur
h. L'interopérabilité de gestion financière; i. La gestion de la sécurité; j. L'évolutivité pendant la durée du contrat existant; et k. La gestion des documents.	
5. Outre les fonctionnalités identifiées à l'appui de la question 4 ci-dessus, la solution proposée comporte-t-elle d'autres fonctionnalités ou caractéristiques non énumérées ci-dessus qui, selon le répondant, pourraient intéresser EDSC?	
6. Indiquez comment le travail de développement sera effectué (par exemple, avec des capacités internes ou en sous-traitance) et, en cas de sous-traitance, qui conservera la propriété des codes sources de développement.	
7. Indiquez s'il existe des limitations quant au nombre de transactions pouvant être gérées par la solution que vous proposez, sur une base quotidienne ou par un seul utilisateur.	
8. Identifiez les exigences en matière de disponibilité pour que la solution fonctionne de manière optimale.	
9. Identifiez l'approche fournie aux clients pour la solution que vous proposez en termes de : a) La mise en œuvre; b) Personnalisation c) Formation; d) Documentation pour l'utilisateur et le système; et e) Soutien.	
10. Fournissez des détails sur le lieu d'hébergement de la solution et sur votre politique de conservation des données (par	

Question	Informations sur le fournisseur
exemple, où les données sont-elles stockées, sur des serveurs locaux, sur des services en nuage, etc.	
11. Décrivez l'allocation de sécurité des données de votre solution et indiquez si votre entreprise a obtenu des audits informatiques conformes aux normes du gouvernement fédéral canadien. Identifiez les certifications de sécurité et les normes d'attestation (FedRAMP, ISO, SOC, etc.) dont disposent les organisations. Pour plus d'informations sur les normes de sécurité pour l'informatique en nuage exigées par le gouvernement du Canada, voir l'annexe B jointe à la présente demande de renseignements.	
12. Indiquez le modèle de licence qui serait nécessaire pour la solution que vous proposez. La durée du contrat est-elle généralement minimale ou maximale?	
13. Décrivez l'approche du cycle de vie annuel du logiciel qui sera recommandée pour la solution proposée et la façon dont le cycle de vie du produit sera déterminé. Indiquez comment les clients sont informés et le type de notification préalable qu'ils reçoivent.	
14. Décrivez l'environnement technique dans lequel la solution proposée fonctionne de manière optimale.	

A2. Questions spécifiques relatives aux exigences non techniques et techniques

Question	Informations sur le fournisseur
1. Identifiez le type d'utilisateurs et la manière dont ils accéderaient à la solution proposée à la lumière de la solution actuelle d'EDSC.	
2. Décrivez les spécialistes en la matière, tels que les traducteurs/réviseurs/spécialistes linguistiques, qui utilisent généralement la solution proposée et comment ils pourraient fournir les types de services identifiés à l'article 6.0 de l'appel d'offres.	
3. Fournissez une description de toutes les caractéristiques et, si possible, les spécifications du produit pour la composante « mémoire de traduction » de la solution proposée, y compris ce qui est inclus, comment on y accède, etc.	
4. Décrivez toutes les caractéristiques et, si possible, les spécifications du produit pour la plate-forme de gestion des demandes de la solution proposée et indiquez comment la gestion des demandes peut être gérée de manière typique dans le cadre de la solution proposée.	
5. Fournissez une description de toutes les fonctionnalités et, si possible, les spécifications du produit pour la gestion du flux de travail de la solution proposée.	
6. Identifiez les outils inclus dans la solution proposée pour permettre au personnel non linguistique d'effectuer, par exemple, des traductions rapides.	
7. Identifiez la (les) langue(s) dans laquelle (lesquelles) le support, la documentation utilisateur et système, les tutoriels/la formation utilisateur et les écrans utilisateur peuvent être utilisés sans développement supplémentaire de la solution.	

Question	Informations sur le fournisseur
8. Décrivez la fonctionnalité que la solution proposée offre pour garantir la qualité des résultats des utilisateurs, par exemple en mettant en évidence les demandes incomplètes, etc.	
9. Décrivez les fonctions d'audit et de présentation de rapport disponibles dans le cadre de la solution proposée.	
10. Confirmez si la solution proposée respecte respecte les directrices pour l'accessibilité du contenu Web, version 2.2 niveau AA (WCAG 2.2 AA). Si possible, identifiez le délai dans lequel les technologies de l'information et de la communication (TIC) de la solution ont été accédées par un tiers ou un spécialiste de l'accessibilité qualifié.	
11. Identifiez si le répondant dispose de services professionnels pour aider à la mise en œuvre de la solution proposée, l'aider à apporter les modifications requises à la solution et répondre aux exigences en matière d'accessibilité.	
12. Fournir une description du mécanisme de rétroaction en place pour recevoir les billets liés à l'utilisation de la solution, les défauts possibles, etc. et les niveaux de service pour les résoudre. Confirmez la langue dans laquelle le processus fonctionnera.	
13. Identifiez s'il y a des composantes ou la solution proposée pour lesquelles le répondant n'a pas de contrôle sur le code source.	

Annexe B — Tableau 1 — Obligations de sécurité pour les services commerciaux d'informatique en nuage (notamment, allant jusqu'au niveau Protégé B)

(À des fins de renseignements seulement)

Généralités

1.1 *Objet*

La présente annexe a pour objet d'énoncer les obligations de l'entrepreneur relatives à la bonne gestion des données du Canada, y compris la protection contre la modification, l'accès ou l'exfiltration non autorisés, conformément à l'Accord, à la présente annexe et aux mesures de sécurité de l'entrepreneur (collectivement, les « **obligations en matière de sécurité** »).

1.2. *Déroulement des obligations de sécurité*

Les obligations de l'entrepreneur contenues dans les présentes obligations de sécurité doivent être réparties par l'entrepreneur entre tous les sous-traitants principaux ou secondaires, selon le cas.

1.3 *Gestion du changement*

L'entrepreneur doit, tout au long du contrat, prendre toutes les mesures nécessaires pour mettre à jour et maintenir les exigences en matière de sécurité, au besoin, afin de se conformer aux pratiques exemplaires en matière de sécurité et aux normes de l'industrie énoncées dans la présente annexe.

L'entrepreneur doit informer le Canada de tous les changements qui dégradent matériellement ou qui peuvent avoir un effet négatif sur les offres de services infonuagiques dans le cadre du présent contrat, y compris les changements ou les améliorations technologiques, administratives ou d'autres types. L'entrepreneur convient d'offrir toutes les améliorations qu'il propose à ses clients en général dans le cadre de son offre de service standard, sans frais supplémentaires pour le Canada.

Reconnaissance

Les parties reconnaissent que :

(a) Les données du Canada sont soumises à ces obligations de sécurité.

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

(c) L'entrepreneur ne doit pas avoir ou tenter d'obtenir la garde des données du Canada ni permettre au personnel des services en nuage d'accéder aux données du Canada avant la mise en œuvre des exigences relatives à la sécurité, comme l'exige la présente annexe, au plus tard à la date d'attribution du contrat.

(d) Les obligations de sécurité s'appliquent aux **services commerciaux d'informatique en nuage** (notamment, allant jusqu'au niveau Protégé B/Intégrité moyenne, Disponibilité moyenne ou Blessure moyenne), sauf indication contraire.

Protection des données du Canada

(1) L'entrepreneur doit protéger les données du Canada contre l'accès, la modification ou l'exfiltration non autorisés. Cela comprend la mise en œuvre et le maintien de mesures de sécurité techniques et organisationnelles appropriées, y compris des politiques, des procédures et des contrôles de sécurité en matière de sécurité de l'information, afin de préserver la confidentialité, l'intégrité et la disponibilité des données du Canada.

Rôles et responsabilités en matière de sécurité

(1) L'entrepreneur doit clairement délimiter les rôles et les responsabilités de l'entrepreneur et du Canada en ce qui concerne les contrôles et les caractéristiques de sécurité des services infonuagiques. Cela inclut, au minimum, les rôles et les responsabilités pour : (i) la gestion des comptes; (ii) la protection des limites; (iii) la sauvegarde des biens et des systèmes d'information; (iv) la gestion des incidents; (v) la surveillance des systèmes; et (vi) la gestion des vulnérabilités.

(2) L'entrepreneur doit fournir au Canada un document à jour qui délimite les rôles et les responsabilités : (i) au moment de l'attribution du contrat; (ii) sur une base annuelle; (iii) lorsqu'il y a des variations importantes de ces rôles et responsabilités à la suite d'une modification des services infonuagiques; ou (iv) à la demande du Canada.

Assurance par une tierce partie : Certifications et rapports

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

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

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

(b) ISO/IEC 27017:2015 Technologies de l'information — Techniques de sécurité — Code de bonne pratique pour les contrôles de sécurité de l'information basés sur ISO/IEC 27002 pour les services infonuagiques, obtenu par un organisme de certification accrédité (ou des versions ultérieures); ET

(c) Contrôles 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-traitant applicable; ii) mentionner la date de certification de l'entrepreneur ou du sous-traitant et l'état de cette certification; et iii) dresser

la liste des services visés par le rapport de certification. Si des exclusions sont relevées, ou s'il est nécessaire de séparer des services de sous-traitants 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 et fournir au Canada des preuves à l'appui des mesures correctives prises ou une confirmation du vérificateur que les problèmes ont été corrigés à la satisfaction du vérificateur.

(5) Chaque rapport SOC 2 type II doit avoir été réalisé 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 SOC 2 Type II pour toute la durée du contrat. L'entrepreneur doit fournir, au moins une fois par année et rapidement à la demande du Canada, tous les rapports ou documents pouvant être raisonnablement exigés pour démontrer que l'entrepreneur possède des certifications actuelles.

Vérification de la conformité

(1) L'entrepreneur doit effectuer les vérifications de confidentialité et de sécurité portant sur la sécurité des ordinateurs, l'environnement informatique et les centres de données physiques qu'il utilise pour traiter et protéger les données du Canada, 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; et

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

(2) Chaque vérification donnera lieu à la production d'un rapport qui doit être mis à la disposition du Canada. Le rapport de vérification doit indiquer clairement toutes les constatations importantes faites par le tiers vérificateur. 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. Ceci s'applique également au cas où l'entrepreneur est un fournisseur SaaS ou PaaS qui utilise des centres de données physiques fournis par un fournisseur IaaS tiers.

Programme d'évaluation de la sécurité des TI du fournisseur de services infonuagiques (FSI)

(1) L'entrepreneur doit démontrer qu'il respecte les exigences de sécurité sélectionnées dans l'Annexe B — Profil de contrôle de la sécurité infonuagique — MOYEN — Guide sur la catégorisation de la sécurité des services fondés sur l'infonuagique (ITSP.50.103) (https://www.cyber.gc.ca/fr/orientation/guide-sur-la-categorisation-de-la-securite-des-services-fondes-sur-linfonuagique) selon la portée des services infonuagiques fournis par l'entrepreneur. La conformité doit être démontrée par la mise en correspondance des contrôles de sécurité avec les certifications de l'industrie applicables énoncées ci-dessous, puis validée au moyen d'évaluations de tiers indépendants.

La conformité sera validée et vérifiée par l'entremise du Processus d'évaluation de la sécurité des technologies de l'information (ITSM.50.100) s'appliquant aux fournisseurs de services infonuagiques (FSI) du Centre canadien pour la cybersécurité (CCC) (https://www.cyber.gc.ca/fr/orientation/processus-devaluation-de-la-securite-des-technologies-de-linformation-sappliquant-aux).

L'entrepreneur doit démontrer qu'il a participé au processus en réussissant l'intégration, la réalisation et l'achèvement du programme. Il lui faudra notamment produire les documents suivants :

(i) Une copie du rapport d'évaluation le plus récent fourni par le Canada; et
(ii) Une copie du rapport sommaire le plus récent fourni par le Canada.

L'entrepreneur qui souhaite en savoir plus sur le processus d'évaluation STI du CCC visant les FSI doit communiquer avec le service du gouvernement du Canada chargé de la passation des marchés.

En tout temps, il incombe à l'entrepreneur des services infonuagiques proposés d'avertir le CCC lorsque des changements importants sont apportés à la prestation des services de sécurité des TI associée à son offre.

(2) Dans le cas où l'entrepreneur est un fournisseur d'IaaS approuvé par le gouvernement du Canada qui se conforme déjà aux dispositions de la section 5 — Assurance par une tierce partie et des paragraphes (1) et (2) de la section 7 — Programme d'évaluation de la sécurité des TI du fournisseur de services infonuagiques (FSI), le fournisseur de SaaS doit présenter au Canada une copie d'un courriel envoyé par le Centre canadien pour la cybersécurité (CCC) confirmant que le soumissionnaire a terminé le processus d'évaluation STI du CCC visant les FSI. Le courriel doit préciser que le FSI a été évalué par le processus d'évaluation STI du CCC visant les FSI et qu'il a reçu un rapport final concernant l'évaluation. Vous pouvez envoyer vos questions par courriel au CCC à l'adresse contact@cyber.gc.ca.

Protection des données

(1) L'entrepreneur doit :

(a) Mettre en œuvre le chiffrement des données inactives pour tous les services infonuagiques 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 13 — 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 13 — Protection cryptographique et à la section 21 — Sécurité des réseaux et des communications;

(2) L'entrepreneur doit :

(a) Mettre en place des contrôles de sécurité qui restreignent l'accès administratif aux données et aux systèmes du Canada par l'entrepreneur et qui permettent d'exiger l'approbation 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 pour s'assurer que le personnel de l'entrepreneur n'a pas de droits d'accès permanents ou continuels aux données du Canada, et que l'accès est 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.

(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 doit s'assurer que tout traitement effectué hors du Canada, y compris le déplacement ou la transmission de copies approuvées des données, a lieu dans les régions de service convenues, sauf s'il a obtenu l'autorisation écrite 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.

Isolement des données

(1) L'entrepreneur doit mettre en place des contrôles visant à assurer un isolement approprié 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 infonuagiques et de l'infrastructure de l'entrepreneur. Cela comprend la mise en œuvre de contrôles 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) (Pour IaaS) La capacité du 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 lui fournir un document qui décrit l'approche permettant d'assurer l'isolement 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.

Emplacement des données

(1) L'entrepreneur doit avoir la capacité 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 30 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; et
(c) Il emploie le chiffrement pour s'assurer qu'aucune donnée n'est écrite sur disque sous une forme non chiffrée, conformément à la section 13 — Protection cryptographique.

(2) L'entrepreneur doit certifier que la prestation et l'approvisionnement des services infonuagiques en vertu du présent contrat proviennent de pays membres de l'Organisation du traité de l'Atlantique Nord (OTAN) (https://www.nato.int/cps/fr/natohq/topics_52044.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 dispose d'un dispositif bilatéral de sécurité industrielle internationale. 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 du PSC (https://www.tpsgc-pwgsc.gc.ca/esc-src/international-fra.html), mis à jour ponctuellement.

(3) L'entrepreneur doit mettre en œuvre la capacité pour le Canada d'isoler les données du Canada hébergées dans des services infonuagiques dans des centres de données géographiquement situés au Canada.

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

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

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

(5) L'entrepreneur des services infonuagiques proposés a l'obligation continue de fournir un avis écrit au Canada lorsque des mises à jour sont apportées à la liste des emplacements physiques qui peuvent contenir des données du Canada.

Transfert et récupération des données

L'entrepreneur doit fournir la capacité, y compris les outils et les services qui permettent au Canada de :

(a) Extraire toutes les données du Canada en ligne, près de la ligne et hors ligne, y compris, mais sans s'y limiter, les bases de données, le stockage d'objets et de fichiers, les configurations de système, les journaux d'activité dans le nuage, le code source hébergé dans un dépôt de code du Canada et les configurations de réseau, de telle sorte que tout utilisateur final du Canada puisse utiliser ces instructions pour migrer d'un environnement à un autre environnement; et

(b) Transférer en toute sécurité toutes les données du Canada, y compris les données de contenu et les métadonnées associées, dans un format lisible et utilisable par machine, y compris le format CSV, et conformément aux lignes directrices de Bibliothèque et Archives Canada sur les formats de fichier pour le transfert des ressources d'information de valeur durable (https://bibliotheque-archives.canada.ca/fra/services/gouvernement-canada/information-disposition/lignes-directrices-information/Pages/lignes-directrices-formats-fichier-ressources-documentaires.aspx).

Disposition des données et renvoi des dossiers au Canada

(1) L'entrepreneur doit éliminer ou réutiliser de façon sécuritaire les ressources (p. ex. équipement, stockage de données, fichiers et mémoire) qui contiennent les données du Canada et s'assurer que les données stockées antérieurement ne peuvent être consultées par d'autres clients après avoir été libérées. Cela comprend toutes les copies des données du Canada qui sont effectuées par réplication à des fins de haute disponibilité et de reprise après sinistre. L'élimination ou la réutilisation des ressources par l'entrepreneur doit être harmonisée à l'une des pratiques suivantes :
(i) National Industrial Security Program Operating Manual (DoD 5220.22-M6);ii) Guidelines for Media Sanitization (NIST SP 800-88); ou iii) Effacement et déclassification des supports d'information électroniques (CST ITSG-06).. À la demande du Canada, l'entrepreneur doit fournir un document décrivant son processus d'élimination ou de réutilisation des ressources.

(2) L'entrepreneur doit fournir au Canada une confirmation écrite démontrant l'effacement, la purge ou la destruction réussie de toutes les ressources, selon le cas, et la capacité d'empêcher la réinstallation de tout système enlevé ou détruit, des capacités (logiciel ou processus), des donnée ou d'instance d'informations une fois que le Canada cesse d'utiliser les services infonuagiques.

Protection cryptographique

L'entrepreneur doit :

(a) Configurer toute cryptographie utilisée pour mettre en œuvre des mesures de confidentialité ou d'intégrité, ou utilisée dans le cadre d'un mécanisme d'authentification (par exemple, solutions RPV, TLS, modules logiciels, ICP et jetons d'authentification, le cas échéant), conformément aux algorithmes cryptographiques approuvés par le Centre de la sécurité des télécommunications (CST) et à la taille des paramètres cryptographiques, à la longueur des clés et aux périodes de chiffrement des clés, comme spécifié dans les documents « Algorithmes cryptographiques pour l'information non classifié, protégé A et protégé B » (ITSP.40.111) et « Conseils sur la configuration sécurisée des protocoles réseau » (ITSP.40.062) et restent conformes à toute version ultérieure publiée sur https://cyber.gc.ca/;

(b) Utiliser des algorithmes cryptographiques approuvés par le CST et validés par le programme de validation des modules cryptographiques (PVMC) (https://www.cyber.gc.ca/fr/outils-services/programme-validation-modules-cryptographiques-pvmc), avec des tailles de paramètres cryptographiques et des longueurs de clés, comme spécifié dans « Algorithmes cryptographiques pour l'information non classifié, protégé A et protégé B » (ITSP.40.111) et rester cohérent avec toutes les versions ultérieures publiées sur https://www.cyber.gc.ca/fr;

(c) Veiller à ce que l'utilisation d'algorithmes cryptographiques, la taille des paramètres cryptographiques, la longueur des clés et les périodes cryptographiques soient configurables et puissent être mises à jour dans les protocoles, les applications et les services afin d'être conformes aux orientations en matière de transition en temps utile pour respecter les dates de transition spécifiées dans les documents « Algorithmes cryptographiques pour l'information non classifié, protégé A et protégé B » (ITSP.40.111) et « Conseils sur la configuration sécurisée des protocoles réseau » (ITSP.40.062) et rester conformes à toutes les versions ultérieures publiées sur le site https://www.cyber.gc.ca/fr. Les contractants doivent soutenir la transition vers une cryptographie à sécurité quantique conformément aux orientations énoncées dans les documents ITSP.40.111 et ITSP.40.062 et leurs versions ultérieures.

(d) Veiller à ce que des modules cryptographiques validés par le programme de validation des modules cryptographiques (PVMC) soient utilisés lorsque la cryptographie est nécessaire, et qu'ils soient mis en œuvre, configurés et exploités conformément à la politique de sécurité des modules cryptographiques figurant sur la liste des modules validés par le PVMC (https://www.cyber.gc.ca/fr/outils-services/programme-validation-modules-cryptographiques-pvmc), en mode approuvé ou autorisé, afin de garantir avec un degré élevé de certitude que le module cryptographique validé par le PVMC fournit les services de sécurité escomptés de la manière escomptée; et

(e) S'assurer que tous les modules cryptographiques utilisés ont une certification PVMC active, à jour et valide. Les produits validés par le PVMC auront des numéros de certificat figurant sur la liste des modules validés par le PVMC (https://www.cyber.gc.ca/fr/outils-services/programme-validation-modules-cryptographiques-pvmc).

Gestion des clés

L'entrepreneur doit fournir au Canada un service de gestion des clés conforme au Guide sur le chiffrement des services infonuagiques (ITSP.50.106) du CCC (https://www.cyber.gc.ca/fr/orientation/guide-sur-le-chiffrement-des-services-infonuagiques-

itsp50106) et leurs versions subséquentes publiées sur le site https://www.cyber.gc.ca/fr, qui comprend :

(a) Capacité à créer/générer et supprimer des clés de chiffrement si exigé par le GC.

(b) Définition et application de politiques spécifiques qui contrôlent la manière dont les clés peuvent être utilisées;

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

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

(e) La capacité d'importer de façon sécuritaire les clés générées, à partir d'un module matériel de sécurité (MMS), géré sur place par le GC, et ce, sans exposition du texte en clair des clés pendant le processus d'importation;

(f) La capacité d'empêcher le fournisseur de services infonuagiques de récupérer des copies en texte clair des clés générées par le GC; et

(g) La capacité de déléguer les privilèges liés à l'utilisation des clés pour leur usage par les services infonuagiques utilisés pour les services gérés par le GC.

Protection des points terminaux

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 relatif à la sécurité générale des serveurs), des points de référence du Centre pour la sécurité internet (CSE) ou d'une norme équivalente approuvée par écrit par le Canada.

Développement sécurisé

L'entrepreneur doit mettre en œuvre un cycle de vie de développement de logiciels et de systèmes qui applique les principes d'ingénierie de la sécurité des systèmes d'information tout au long de leur cycle de vie et dans le développement de logiciels, de sites Web et de services. Ce cycle de vie doit être conforme aux normes et aux pratiques exemplaires du secteur, comme : i) NIST, ii) ISO 27034, iii) ITSG-33, iv) SAFECode ou v) Open Web Application Security Project (OWASP) (p. ex. Application Security Verification Standard [ASVS]) ou une norme équivalente approuvée par le Canada par écrit. 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.

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 infonuagiques, y compris la capacité de configurer :

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

(b) Un accès basé sur les rôles;

(c) Des contrôles de l'accès aux objets stockés; et

(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.

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 OpenID Connect 1.0 (ou versions ultérieures), selon lesquels les identifiants de l'utilisateur final et l'authentification aux services infonuagiques relèvent exclusivement du Canada; et

(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 infonuagiques correspondants.

Gestion de l'accès privilégié

(1) L'entrepreneur doit :

(a) Mettre en œuvre des politiques et des procédures de contrôle d'accès qui traitent de l'intégration, de la désintoxication, de la transition entre les rôles, des examens réguliers de l'accès pour identifier les privilèges excessifs, des limitations et du contrôle de l'utilisation des privilèges d'administrateur;

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

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

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

(e) 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 identifiants, ii) l'utilisation inhabituelle de ces derniers et iii) l'accès et l'exfiltration des mots de passe depuis la base de données, conformément à la version 3 (ou aux versions ultérieures) de la norme ITSP.30.031 du CST (https://www.cyber.gc.ca/fr/orientation/guide-sur-lauthentification-des-utilisateurs-dans-les-systemes-de-technologie-de);

(g) Mettre en œuvre des mécanismes d'authentification multifactorielle pour authentifier les utilisateurs finaux ayant un accès privilégié, conformément à la norme ITSP.30.031 V3 (ou versions ultérieures) du CST (https://www.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 infonuagiques 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 infonuagiques et de l'infrastructure de l'entrepreneur;

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

(m) En cas de cessation d'emploi, résilier ou révoquer les authentifiants et les identifiants d'accès associés à tout membre du personnel des 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 infonuagiques.

Gestion à distance

(1) L'entrepreneur doit gérer et surveiller l'administration à distance de ses services infonuagiques 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 CST (https://www.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) Déconnecter ou désactiver rapidement les connexions non autorisées de gestion à distance ou d'accès à distance;

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

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

Sécurité des réseaux et des communications

L'entrepreneur doit :

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

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

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

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

Consignation et vérification

(1) L'entrepreneur doit mettre en œuvre des pratiques et des contrôles de création et de gestion des journaux pour toutes les composantes des services infonuagiques 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 contrôles de création et de gestion des journaux.

(2) L'entrepreneur doit permettre au Canada d'examiner et d'analyser de façon centralisée les dossiers de vérification de multiples composantes (p. ex. réseau, données, stockage, calcul, etc.) des services infonuagiques utilisés par le Canada., afin de permettre au Canada d'effectuer la surveillance de la sécurité, la production de rapports, l'analyse, l'enquête et la mise en œuvre de mesures correctives, selon les besoins. Il s'agit notamment de la possibilité pour le Canada de :

(a) enregistrer et détecter les événements de vérification tels que (i) les tentatives réussies et infructueuses de connexion à un compte, (ii) la gestion des comptes, (iii) l'accès aux objets et la variation des politiques, (iv) les fonctions de privilège et le

suivi des processus, (v) les événements système, (vi) la suppression de données, et conformément aux directives du Canada en matière de consignation des événements (https://www.canada.ca/fr/gouvernement/systeme/gouvernement-numerique/securite-confidentialite-ligne/guide-sur-la-consignation-evenements.html);

(b) enregistrer dans les journaux (ou fichiers journaux) les événements de vérification qui sont synchronisés et horodatés en temps universel coordonné (UTC) et protégés contre tout accès, modification ou suppression non autorisés pendant qu'ils sont en transit et au repos;

(c) fournir des alertes en temps réel en cas d'échec des événements de vérification au personnel habilité à y remédier; et

(d) séparer les incidents de sécurité et les journaux pour les différents comptes du Canada afin de permettre au Canada de surveiller et de gérer les événements à l'intérieur de son périmètre qui affectent son instance d'un service infonuagique IaaS, PaaS ou SaaS qui lui est fourni par l'entrepreneur ou un sous-traitant.

(3) L'entrepreneur doit donner au Canada les capacités 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 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 infonuagiques qu'il utilise, pour appuyer les activités du GC, y compris la surveillance des services infonuagiques et la divulgation électronique et les mises en suspens pour des raisons juridiques.

(4) Pour le SaaS, l'entrepreneur doit fournir des API qui permettent de :

(a) Inspecter et interroger les données inactives dans les applications SaaS;

(b) Évaluer les événements tels que l'accès et le comportement des utilisateurs, l'accès et le comportement des administrateurs, et les modifications de l'accès à l'API de tiers, stockées dans les registres d'applications SaaS.

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 infonuagiques 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) Effectuer régulièrement des analyses de vulnérabilité et des essais de pénétration de l'infrastructure de l'entrepreneur et des emplacements de services, dans le but de cerner les lacunes et de prendre des mesures correctives afin d'empêcher l'accès non autorisé à des renseignements sensibles, le contournement des contrôles d'accès et l'élévation des privilèges, ainsi que l'exploitation des vulnérabilités pour obtenir l'accès à des systèmes ou à des renseignements.

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

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

(e) Détecter l'utilisation et l'accès non autorisés à tous les services infonuagiques, données et composants afférents aux services infonuagiques IaaS, PaaS ou SaaS du Canada;

(f) Gérer et appliquer les correctifs et les mises à jour liés à la sécurité de manière opportune et systématique afin d'atténuer les vulnérabilités et de corriger tout problème signalé publiquement dans les services infonuagiques ou les bibliothèques que les services infonuagiques utilisent, et donner des préavis de correctif conformément aux engagements convenus relatifs au niveau de service;

(g) Répondre aux menaces et aux attaques contre les services infonuagiques de l'entrepreneur, les contenir et veiller à la récupération; et

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

(2) Les services infonuagiques publics de l'entrepreneur doivent permettre de copier les données des applications des services du GC (pour les services IaaS, PaaS et SaaS) et le trafic réseau du GC (pour les services IaaS et PaaS) hébergés en nuage et de les acheminer vers un emplacement prédéterminé (dans le nuage ou dans les locaux du GC).

(3) Pour le SaaS, les services infonuagiques de l'entrepreneur doivent permettre au Canada de déployer et d'exploiter un logiciel de sécurité pour effectuer une surveillance avancée et des mesures d'atténuation des cybermenaces pour les services infonuagiques du Canada pour les composantes gérées par le Canada seulement.

Gestion des incidents de sécurité

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

(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; ou ii) NIST SP800-612, Computer Security Incident Handling Guide; ou iii) Plan de gestion des événements de cybersécurité du gouvernement du Canada (PGEC GC).

(https://www.canada.ca/fr/gouvernement/systeme/gouvernement-numerique/securite-confidentialite-ligne/gestion-securite-identite/plan-gestion-evenements-cybersecurite-gouvernement-canada.html); ou (iv) d'autres pratiques exemplaires tirées des normes de l'industrie, si le Canada détermine, à sa discrétion, qu'elles satisfont aux exigences du Canada en matière de sécurité.

(b) Des processus et des procédures documentés sur la façon dont l'entrepreneur détectera les incidents de sécurité de l'information, y donnera suite, les corrigera, les signalera et en fera part au Canada, notamment : i) La portée des incidents 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 liés aux incidents liés à la sécurité de l'information, conformément aux procédures de notification énoncées dans le PGSC du 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) les mesures correctives applicables en cas d'incidents liés à la sécurité de l'information.

(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 préautorisés du client (p. ex. le Centre canadien pour la cybersécurité ou d'autres organisations approuvées par le GC) et 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 des 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) Des procédures de réponse aux demandes de preuves numériques potentielles ou d'autres renseignements se trouvant dans l'environnement des services infonuagiques et conformes aux normes et aux meilleures pratiques du secteur, notamment la norme ISO 22095:2020 Chaîne de contrôle — Terminologie générale et modèles (https://www.iso.org/fr/standard/72532.html), y compris les procédures judiciaires et les mesures de protection appropriées pour :

(i) le maintien d'une chaîne de contrôle pour les renseignements de vérification, et
(ii) la collecte, la conservation et la présentation de preuves qui démontrent l'intégrité de ces dernières.

(2) Dans les dix jours suivant la date d'entrée en vigueur du contrat, l'entrepreneur doit fournir un document décrivant sa procédure de réponse aux incidents de sécurité, y compris les coordonnées des personnes-ressources. Ce processus, y compris les coordonnées des personnes-ressources, doit demeurer à jour et, à tout le moins, être validé chaque année et être approuvé par le Canada.

(3) L'entrepreneur doit :

(a) Travailler avec les centres des opérations de sécurité du Canada (p. ex. le SOC du GC, les équipes ministérielles de sécurité des TI) et les principaux intervenants du PGEC GC (c.-à-d. le CCC et le Secrétariat du Conseil du Trésor du Canada [SCT]), en vue du confinement et de l'élimination des incidents de sécurité, et de la reprise des activités conformément au processus d'intervention en cas d'incident 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, et les enregistrements des activités liées à la gestion de l'incident de sécurité, y compris les communications internes et externes (par exemple, dans le cas d'un logiciel de rançon, toutes les communications, y compris les demandes de rançon, etc.) Ces informations doivent être fournies au Canada sur demande; et

(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.

(4) Pour appuyer les enquêtes de sécurité, le Canada peut exiger de l'entrepreneur des preuves judiciaires 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 ans après la fin de l'enquête ou les fournir au Canada pour qu'ils soient conservés;

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

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

(d) soutenir l'investigation informatique; et

(e) conserver les dossiers juridiques pour répondre aux besoins des enquêtes et des demandes judiciaires.

(5) Si l'entrepreneur fait appel à une entreprise externe pour ses activités d'intervention en cas d'incident, il doit veiller à ce que les dispositions énoncées dans le présent *article 25 — Gestion des incidents de sécurité et dans l'article 26 — 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.

Intervention en cas d'incident de sécurité

(1) L'entrepreneur doit alerter et informer promptement le Canada (par téléphone ou par courriel) de toute compromission, atteinte à la sécurité ou 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 ou atteinte à la sécurité et détermine qu'elle peut entraîner la destruction, la perte, l'altération, la divulgation non autorisée des données ou des données personnelles du client, ou encore l'accès aux données ou aux données personnelles du client, pendant le traitement par l'entrepreneur (chacun étant un « incident de sécurité »), l'entrepreneur doit rapidement et sans tarder i) informer le Canada de cet incident de sécurité; ii) mener une enquête et fournir au Canada des renseignements détaillés sur cet incident de sécurité; iii) prendre les mesures raisonnables pour remédier aux causes et atténuer les dommages découlant de l'incident de sécurité.

(3) À la demande du Canada, les entrepreneurs doivent signaler les incidents majeurs à la police compétente.

Fuite d'information

(1) L'entrepreneur doit disposer d'un processus documenté décrivant son approche en cas d'incident de fuite d'information. Le processus doit être aligné sur : i) les directives de la section IR-9 intitulée Intervention en cas de fuite d'information du document ITSG-33, ou ii) sur 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; et

(c) Un processus d'identification des systèmes susceptibles d'avoir été contaminés par la suite et toute autre mesure prise pour éviter une nouvelle 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.

Test de sécurité et validation

(1) L'entrepreneur doit disposer d'un processus permettant d'effectuer une analyse de vulnérabilité ou un test de pénétration non perturbateur et non destructeur des services infonuagiques hébergeant les données du Canada. Cela comprend la capacité d'effectuer régulièrement des analyses internes et externes liées à la location du GC, et lorsqu'il y a des variations importantes à la plateforme principale, afin de repérer toute vulnérabilité potentielle du système liée à la location du GC en effectuant :

i. des analyses de vulnérabilité;
ii. des analyses d'applications web; et
iii. des tests de pénétration.

(2) L'entrepreneur doit élaborer un plan d'action et des jalons pour documenter toutes les mesures correctives prévues pour corriger les faiblesses ou les lacunes de la plateforme principale afin de réduire ou d'éliminer les vulnérabilités connues du système, ou celles qui pourraient être liées aux services infonuagiques hébergeant les données du Canada et à l'exploitation de la tendance du GC.

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

(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 infonuagiques configurés par le Canada.

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 qui participe à la prestation de services infonuagiques 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 du Conseil du Trésor sur le filtrage de sécurité (https://www.tbs-sct.canada.ca/pol/doc-fra.aspx?id=28115) ou utiliser un équivalent acceptable convenu par le Canada.

(3) À la demande du Canada, l'entrepreneur doit produire un document qui décrit son processus de filtrage de sécurité du personnel. Le processus doit au moins prévoir

(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 infonuagiques;

(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 des employés, lorsque les rôles des employés et des sous-traitants changent, et de façon continue, pour s'assurer que les employés et les sous-traitants comprennent, connaissent et assument leurs responsabilités en matière de sécurité de l'information;

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

(e) L'approche de détection des employés en place potentiellement malveillants et les contrôles mis en œuvre pour atténuer le risque d'accès aux données du GC ou de dommage à la fiabilité des services infonuagiques hébergeant les données du Canada.

Sécurité physique (centre de données/installations)

(1) L'entrepreneur doit mettre en œuvre des mesures de sécurité physique qui assurent la protection des installations informatiques et des actifs des systèmes d'information sur lesquels les données du Canada sont stockées et traitées contre toute forme d'altération, de perte, de

dommage et de saisie. La protection physique de toutes les installations qui hébergent des données du Canada doit être appliquée selon une approche adaptée fondée sur les risques et reposant sur la prévention, la détection, l'intervention et la récupération en matière de sécurité physique, alignée sur les contrôles de sécurité physique et les pratiques de la norme de sécurité opérationnelle du Conseil du Trésor sur la sécurité physique (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 TI;

(iii) Le contrôle de la maintenance de tous les systèmes d'information et de leurs composantes 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 infonuagiques 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; et

(ix) L'exécution de contrôles de sécurité continus à la limite des points de service et des installations afin de déceler toute exfiltration non autorisée d'information ou de composantes de systèmes.

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

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

Gestion des risques de la chaîne d'approvisionnement

(1) L'entrepreneur doit prendre des mesures de protection pour atténuer les menaces et les vulnérabilités associées à la chaîne d'approvisionnement des services de TI en vue de

préserver la confiance en ce qui concerne la sécurité des sources des systèmes d'information et les composants de TI servant à offrir les services infonuagiques. En font notamment partie la protection tout au long du cycle de développement des systèmes par la conception et la mise en œuvre de contrôles visant à atténuer et à contenir les risques liés à la sécurité des données par une séparation adéquate des tâches, un accès établi selon les rôles et un accès qui suit le principe du privilège minimal pour tout le personnel au sein de la chaîne d'approvisionnement; la sensibilisation aux menaces, la formation du personnel chargé des acquisitions aux menaces, aux risques et aux contrôles de sécurité requis; et l'obligation pour les entités de la chaîne d'approvisionnement de mettre en œuvre les mesures de protection nécessaires.

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

(i) ISO/IEC 27036 Technologies de l'information — Techniques de sécurité — Sécurité d'information pour la relation avec le fournisseur (parties 1 à 4);

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

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

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

(a) Présenter une preuve selon laquelle l'approche et le plan de gestion des risques de la chaîne d'approvisionnement ont été évalués et validés par un tiers indépendant certifié selon les exigences de l'AICPA, de CPA Canada ou du régime de certification ISO.

OU

(b) Fournir au Canada une copie du plan de gestion des risques liés à la chaîne d'approvisionnement sur une base annuelle ou sur demande.

(4) Dans le cas où l'entrepreneur est un fournisseur SaaS qui utilise un fournisseur IaaS approuvé par le GC et qui se conforme déjà aux exigences de l'article 31 — Gestion des risques de la chaîne d'approvisionnement, dans les 90 jours suivant l'attribution du contrat, le fournisseur SaaS qui fait appel à un fournisseur IaaS
doit fournir une liste de produits de technologie de l'information et de la communication (TIC) décrivant l'équipement de TIC déployé dans l'environnement du fournisseur IaaS approuvé par le GC aux fins d'examen de l'intégrité de la chaîne d'approvisionnement. Cet examen de l'intégrité de la chaîne d'approvisionnement sera effectué au plus tôt tous les trois ans.

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

Programme de sécurité industrielle — Exigences relatives à la sécurité pour les fournisseurs canadiens

(1) L'entrepreneur/offrant doit détenir en permanence, pendant la réalisation du contrat, de l'offre à commandes ou de l'arrangement en matière d'approvisionnement, une attestation de vérification d'organisation désignée (VOD) en vigueur, ainsi qu'une cote de protection des documents approuvés au niveau PROTÉGÉ B, délivrée par le Programme de sécurité des contrats (PSC) de Travaux publics et Services gouvernementaux Canada (TPSGC).

(2) Les membres du personnel de l'entrepreneur/offrant devant accéder à des renseignements, à des biens ou à des lieux de travail de niveau PROTÉGÉ doivent TOUS détenir une cote de sécurité du personnel valide au niveau SECRET ou FIABILITÉ selon la classification de sécurité, délivrée 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 approbation aura été accordée, ces tâches pourront être exécutées au niveau PROTÉGÉ B, y compris un lien électronique au niveau PROTÉGÉ B.

(4) Les contrats de sous-traitance qui contiennent des exigences en matière de sécurité NE DOIVENT PAS être attribués sans l'autorisation écrite préalable du PSC de TPSGC.

(5) L'entrepreneur/offrant doit se conformer aux dispositions :

(a) de la liste de vérification des exigences relatives à la sécurité et guide de sécurité (le cas échéant), joints aux annexes A et B;

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

(c) Site Web du PSC Exigences de sécurité des contrats du gouvernement du Canada disponibles à l'adresse suivante : 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.

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 dans un État autre que le Canada et qui livrent ou exécutent à l'extérieur du Canada les services infonuagiques décrits dans les solutions d'infonuagique, en plus des exigences en matière de confidentialité et de sécurité. Ces exigences en matière de sécurité s'ajoutent aux exigences figurant dans la section intitulée Protection et sécurité des données stockées dans des bases de données.

(1) **L'entrepreneur ou le sous-traitant** atteste que la livraison et a prestation des services infonuagiques prévus par le présent contrat doit provenir d'un pays membre de l'Organisation du Traité de l'Atlantique Nord (OTAN), de l'Union européenne (UE) ou d'un pays avec lequel le Canada a conclu une entente internationale bilatérale sur la sécurité. 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 et telle que mise 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, exerce ses activités et est autorisé à faire des affaires. Le destinataire étranger
L'entrepreneur ou le sous-traitant 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 commencer les travaux, les services ou les prestations avant que l'autorité de sécurité désignée (ASD) canadienne ne se soit assurée que toutes les conditions relatives aux exigences de sécurité du contrat ont été remplies. La confirmation de l'ASD canadienne doit être fournie, par écrit, à l'entrepreneur destinataire étranger dans un formulaire d'attestation, afin de confirmer la conformité et l'autorisation d'exécuter les services.

(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 sur les 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 permettraient 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.canada.ca/pol/doc-fra.aspx?id=28115) ou doit utiliser des mesures équivalentes acceptables convenues par le Canada.

(7) L'information et les biens **PROTÉGÉS PAR LE CANADA** fournis à l'entrepreneur ou au sous-traitant destinataire étranger ou produits par **l'entrepreneur ou sous-traitant** destinataire étranger :

i. ne doivent pas être divulgués à un autre gouvernement, à une autre personne ou à une autre entreprise ou à un représentant de l'un ou de l'autre qui ne soit pas directement lié à l'exécution du contrat, sans l'autorisation écrite préalable du gouvernement.du Canada. Ce consentement doit être obtenu auprès de

l'ADS canadienne en collaboration avec l'autorité contractante; et

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

(8) L'entrepreneur/offrant ne doit pas retirer les informations ou les biens protégés du ou des sites de travail identifiés, et l'entrepreneur/offrant doit s'assurer que son personnel est informé de cette restriction et 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 bénéficiaire doit immédiatement signaler à l'ADS canadienne tous les cas dans lesquels il est connu ou il y a des raisons de soupçonner que des informations/biens PROTÉGÉS PAR LE CANADA dans le cadre du présent contrat ont été compromis.

(12) L'entrepreneur étranger bénéficiaire doit fournir aux informations/biens PROTÉGÉS PAR LE CANADA un niveau de protection non moins aussi rigoureux que celui fourni par le gouvernement du Canada, conformément aux politiques nationales, à la législation et à la réglementation en matière de sécurité nationale et aux prescriptions de l'ADS canadienne.

(13) À l'achèvement des travaux, l'entrepreneur bénéficiaire étranger doit retourner au gouvernement du Canada tous les renseignements ou les biens PROTÉGÉS PAR LE CANADA fournis ou produits en vertu du présent contrat, y compris tous les renseignements ou les biens PROTÉGÉS PAR LE CANADA, communiqués à ses sous-traitants ou produits par eux.

(14) L'entrepreneur bénéficiaire étranger qui a besoin d'accéder à des informations/biens PROTÉGÉS PAR LE CANADA ou à des sites canadiens à accès restreint, dans le cadre de

ce contrat, doit soumettre une demande d'accès au site au responsable de la sécurité de Nom du ministère/de l'organisation du Canada.

(15) L'entrepreneur bénéficiaire étranger NE DOIT PAS utiliser ses systèmes de technologie de l'information (TI) pour traiter, produire ou stocker électroniquement sur un système informatique et transférer via une liaison internet toute information PROTÉGÉE B PAR LE CANADA, tant que l'autorisation de le faire n'a pas été confirmée par l'ADS canadienne.

(16) Les contrats de sous-traitance qui contiennent des exigences en matière de 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 bénéficiaire 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 bénéficiaire 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.

(19) L'entrepreneur**/sous-traitant** bénéficiaire étranger doit se conformer aux dispositions de la liste de contrôle des exigences de sécurité jointe aux annexes B et C.

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

(21) Le Canada a le droit de rejeter toute demande présentée séparément et indépendamment de l'autorisation prévue dans le présent contrat relativement à la prestation de services infonuagiques par l'entrepreneur pour accéder électroniquement aux données **PROTÉGÉES PAR LE CANADA** liées aux services infonuagiques, les traiter, les produire, les transmettre ou les stocker dans tout autre pays s'il y a des raisons de s'inquiéter de la sécurité, de la protection de la vie privée ou de l'intégrité de l'information.

Transport physique et transmission des informations

(1) L'entrepreneur doit mettre en œuvre des mesures pour protéger les renseignements du Canada sous forme physique, y compris les biens immobilisés (par exemple, en cours d'utilisation ou de stockage), en transit (par exemple, en cours de transport ou de transmission) et au moyen d'une destruction appropriée. Cela comprend ce qui suit, sans s'y limiter :

(a) Veiller à ce que les dispositifs de stockage de données portables soient correctement sécurisés à tout moment, en fonction du niveau le plus élevé de classification de sécurité des informations qui y sont stockées, dans un conteneur de sécurité approprié tel que défini par le manuel de sécurité industrielle de SPAC, chapitre 5 (https://www.tpsgc-pwgsc.gc.ca/esc-src/msi-ism/chap5-fra.html) et chapitre 8 (https://www.tpsgc-pwgsc.gc.ca/esc-src/msi-ism/chap8-fra.html), et les principes énoncés dans le G1-001 — Guide d'équipement de sécurité de la GRC (https://www.rcmp-grc.gc.ca/physec-secmat/res-lim/pubs/seg/html/home_f.htm) pour

le conteneur de sécurité, et en veillant à ce que le conteneur de sécurité soit protégé par un mot de passe fort et des mécanismes d'authentification;

(b) Chiffrer toutes les informations du Canada stockées sur des dispositifs de stockage de données portables à l'aide d'un module de chiffrement certifié par le programme de validation des modules cryptographiques, et conformément à la section 13 — Protection cryptographique, y compris l'utilisation de produits accrédités par le programme des critères communs;

(c) Veiller à ce que, avant de connecter l'appareil au réseau informatique du Canada en vue de transferts unilatéraux d'informations des réseaux informatiques du Canada vers l'appareil, ce dernier fasse l'objet d'une recherche de logiciels malveillants à chaque fois qu'il est connecté à l'infrastructure informatique du Canada.

(d) Veiller à ce que tous les dispositifs portables utilisés pour transporter les informations du Canada soient nettoyés afin d'empêcher la récupération des informations, conformément aux exigences de nettoyage des supports décrites dans la section 12 (1) — Disposition des données et renvoi des dossiers au Canada.

(2) Les informations protégées sont considérées comme « en cours de transmission » jusqu'à ce qu'elles aient atteint leur destination et aient été livrées au centre de données du contractant ou ouvertes. S'il est ouvert, il doit alors être protégé, conformément à la section 30 — Sécurité physique, et au manuel de sécurité industrielle du SPAC, chapitre 5 (https://www.tpsgc-pwgsc.gc.ca/esc-src/msi-ism/chap5-fra.html) et au chapitre 8 (https://www.tpsgc-pwgsc.gc.ca/esc-src/msi-ism/chap8-fra.html).

(3) L'entrepreneur doit signaler toute perte ou tout vol réel ou suspecté de dispositifs de stockage de données portables, conformément à l'article 26 — Réponse aux incidents de sécurité, et au manuel de sécurité industrielle du SPAC, chapitre 5 (https://www.tpsgc-pwgsc.gc.ca/esc-src/msi-ism/chap5-fra.html) et au chapitre 8 (https://www.tpsgc-pwgsc.gc.ca/esc-src/msi-ism/chap8-fra.html).