



RETURN BIDS TO:

RETOURNER LES SOUMISSIONS À:

Bid Receiving - PWGSC / Réception des
soumissions - TPSGC

11 Laurier St. / 11, rue Laurier

Place du Portage, Phase III

Core 0B2 / Noyau 0B2

Gatineau

Quebec

K1A 0S5

Bid Fax: (819) 997-9776

REQUEST FOR PROPOSAL DEMANDE DE PROPOSITION

Proposal To: Public Works and Government
Services Canada

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

Proposition aux: Travaux Publics et Services
Gouvernementaux Canada

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

Comments - Commentaires

Vendor/Firm Name and Address

Raison sociale et adresse du

fournisseur/de l'entrepreneur

Issuing Office - Bureau de distribution

Middleware division / Division Intergiciels

Terrasses de la Chaudière

4th Floor, 10 Wellington Street

4th etage, 10, rue Wellington

Gatineau

Quebec

K1A 0S5

Title - Sujet IT Cloud Services Request for Proposal - Business Continuity and Emergency Management Application	
Solicitation No. - N° de l'invitation G9292-202457/B	Date 2022-02-21
Client Reference No. - N° de référence du client G9292-202457	
GETS Reference No. - N° de référence de SEAG PW-\$EEM-063-40581	
File No. - N° de dossier 063eem.G9292-202457	CCC No./N° CCC - FMS No./N° VME
Solicitation Closes - L'invitation prend fin at - à 02:00 PM Eastern Daylight Saving Time EDT on - le 2022-04-04 Heure Avancée de l'Est HAE	
F.O.B. - F.A.B. Plant-Usine: <input type="checkbox"/> Destination: <input type="checkbox"/> Other-Autre: <input type="checkbox"/>	
Address Enquiries to: - Adresser toutes questions à: Ferguson, Daniel	Buyer Id - Id de l'acheteur 063eem
Telephone No. - N° de téléphone (343) 543-3961 ()	FAX No. - N° de FAX () -
Destination - of Goods, Services, and Construction: Destination - des biens, services et construction: EMPLOYMENT AND SOCIAL DEVELOPMENT CANADA NCR-RCN - Gatineau 140 PROMENADE DU PORTAGE GATINEAU Quebec J8X4B6 Canada	

Instructions: See Herein

Instructions: Voir aux présentes

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



Item Article	Description	Dest. Code Dest.	Inv. Code Fact.	Qty Qté	U. of I. U. de D.	Unit Price/Prix unitaire FOB/FAM		Delivery Req. Livraison Req.	Del. Offered Liv. offerte
						Destination	Plant/Usine		
4	SaaS Emergency Management Application System	G9292	I - 1	1	Each	\$	\$	See Herein – Voir ci-inclus	

**DEMANDE DE SOUMISSIONS – SYSTÈME D'APPLICATION DE CONTINUITÉ DES ACTIVITÉS
ET DE GESTION DES URGENCES – EMPLOI ET DÉVELOPPEMENT SOCIAL CANADA**

TABLE DES MATIÈRES

DEMANDE DE SOUMISSIONS – SYSTÈME D'APPLICATIONS DE GESTION DES URGENCES – EMPLOI ET DÉVELOPPEMENT SOCIAL	
CANADA	1
PARTIE 1 – RENSEIGNEMENTS GÉNÉRAUX	5
1.1 Introduction	5
1.2 Résumé	5
1.3 Comptes rendus	6
1.4 Conflit d'intérêts	6
PARTIE 2 – INSTRUCTIONS À L'INTENTION DES SOUMISSIONNAIRES	7
2.1 Instructions, clauses et conditions uniformisées	7
2.2 Présentation des soumissions	7
2.3 Ancien fonctionnaire	8
2.4 Demande de renseignements – Demande de soumissions	9
2.5 Lois applicables	9
2.6 Améliorations apportées au besoin pendant la demande de soumissions	9
2.7 Données volumétriques	10
PARTIE 3 – INSTRUCTIONS POUR LA PRÉPARATION DES SOUMISSIONS	10
3.1 Instructions pour la préparation des soumissions	10
3.2 Présentation d'une seule soumission	10
3.3 Section I : Soumission technique	11
3.4 Section II : Soumission financière	13
3.5 Section III : Certifications	13
3.6 Section IV : Exigences d'intégrité de la chaîne d'approvisionnement	13
PARTIE 4 – PROCÉDURES D'ÉVALUATION ET MÉTHODE DE SÉLECTION	14
4.1 Procédures d'évaluation	14
4.2 Évaluation technique	14
4.3 Évaluation financière	15
4.4 Processus d'intégrité de la chaîne d'approvisionnement	16
4.5 Méthode de sélection	16
4.6 Contrôle de validation de la soumission classée au premier rang	17
4.7 Évaluation informatique du meilleur soumissionnaire	18
4.8 Confirmation de l'inscription au Programme d'évaluation de la sécurité des logiciels-services	18
PARTIE 5 – ATTESTATIONS ET RENSEIGNEMENTS SUPPLÉMENTAIRES	19
5.1 Attestations à joindre à la soumission	19
5.2 Attestations préalables à l'attribution du contrat et renseignements supplémentaires	19

PARTIE 6 – SÉCURITÉ, EXIGENCES FINANCIÈRES ET AUTRES EXIGENCES	
6.1 Capacité financière	21
6.2 Exigences liées au Programme de sécurité industrielle concernant les informations en nuage « Protégé B »	23
PARTIE 7 – CLAUSES DU CONTRAT SUBSÉQUENT	
7.1 Besoin	44
7.2 Services	44
7.3 Services professionnels	44
7.4 Intégralité de l'entente	44
7.5 Client	44
7.6 Réorganisation des clients	44
7.7 Durée déterminée et renouvellement automatique	45
7.8 Rigueur dans les délais	45
7.9 Résiliation pour des raisons de commodité	45
7.10 Accès à l'information	46
7.11 Solution	46
7.12 Services	47
7.13 Autorisation des tâches	52
7.14 Base de paiement	54
7.15 Paiement	55
7.17 Certification des Prix	57
7.18 Limitation de la responsabilité	57
7.19 Dispositions générales	57
7.20 Obligations en matière de sécurité	61
7.21 Obligations en matière de confidentialité	75
7.22 Programme de contrats fédéraux pour l'équité en matière d'emploi - Manquement de la part d'entrepreneur	82
7.23 Ordre de priorité des documents	82
7.24 Ressortissants étrangers (entrepreneur canadien)	82
7.25 Ressortissants étrangers (entrepreneur étranger)	82
APPENDICE A - DÉFINITIONS ET INTERPRÉTATIONS	
ANNEXE « A » – ÉNONCÉ DES BESOINS	84
ANNEXE « B » – BASE DE PAIEMENT	89
ANNEXE « C » – LISTE DE VÉRIFICATION DES EXIGENCES RELATIVES À LA SÉCURITÉ	177
ANNEXE « D » – GUIDE DE CLASSIFICATION DE SÉCURITÉ	180
ANNEXE « E » – Processus d'intégrité de la chaîne d'approvisionnement	181
ANNEXE « F » – Information sur la sécurité de la chaîne d'approvisionnement	190
Annexe « G » – Entente de non-divulgaration de SPAC relatif à l'intégrité de la chaîne d'approvisionnement	204

ANNEXE « H » – PROGRAMME D'ÉVALUATION DE LA SÉCURITÉ DES TI DES LOGICIELS-SERVICES : PROCESSUS D'INTÉGRATION	
.....	205
ANNEXE « I » – Accords sur les niveaux de service (ANS) du ANS	205
ANNEXE « J » de la PARTIE 5 DE LA DEMANDE DE SOUMISSIONS	207
ANNEXE « K » FORMULAIRE TPSGC-PWGC 572 – AUTORISATION DE TÂCHE	209
ANNEXE « L » Formulaire d'autorisation de l'éditeur de logiciels-services	211

PARTIE 1 – RENSEIGNEMENTS GÉNÉRAUX

1.1 Introduction

La présente demande de soumissions contient sept (7) parties, ainsi que des pièces jointes et des annexes, et elle est divisée comme suit :

- Partie 1 Renseignements généraux : renferme une description générale du besoin;
- Partie 2 Instructions à l'intention des soumissionnaires : renferme les instructions, les clauses et les conditions relatives à la demande de soumissions;
- Partie 3 Instructions pour la préparation des soumissions : donne aux soumissionnaires des instructions sur la façon de préparer leur soumission;
- Partie 4 Procédures d'évaluation et méthode de sélection : décrit la façon selon laquelle se déroulera l'évaluation et présente les critères d'évaluation auxquels on doit répondre dans la soumission, ainsi que la méthode de sélection;
- Partie 5 Attestations et renseignements supplémentaires : comprend les attestations et les renseignements supplémentaires à fournir.
- Partie 6 Exigences relatives à l'exigences sécurité, financières et autres exigences : comprend des exigences particulières auxquelles les soumissionnaires doivent répondre.

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

Les annexes comprennent l'énoncé des besoins, la base de paiement, les exigences de sécurité, le processus d'intégrité de la chaîne d'approvisionnement, l'entente de non-divulgaration relative à l'intégrité de la chaîne d'approvisionnement, l'accord sur les niveaux de service (ANS) du logiciel-service, l'attestation du Programme de contrats fédéraux pour l'équité en emploi, le formulaire d'autorisation des tâches, ainsi que le processus d'intégration du Programme d'évaluation de la sécurité des TI des logiciels-services.

1.2 Résumé

- (1) La présente demande de soumissions est émise pour répondre à un besoin d'Emploi et Développement social Canada (EDSC) (le « client ») visant l'acquisition d'une solution de système d'applications de gestion des urgences (SAGU) sous forme de logiciel-service. La configuration du système, la formation ainsi que la capacité du Canada d'isoler les biens et les actifs d'information dans des centres de données situés géographiquement au Canada en font partie. Elle vise l'attribution d'un contrat d'un an, en plus de neuf options irrévocables d'un an chacune qui permettront au Canada de prolonger la durée du contrat.

- (2) ESDC est le client initial qui utilisera le SAGU (le logiciel-service). Par ailleurs, la présente demande de soumissions permettra au Canada de mettre la solution de logiciel-service à la disposition de tous les ministères ou de toutes les sociétés d'État (selon la définition de ces termes dans la *Loi sur la gestion des finances publiques*) ou encore de toute autre partie pour le compte de laquelle le ministère des Travaux publics et de l'Approvisionnement du Canada est autorisé à agir, à l'occasion, en vertu de l'article 16 de la *Loi sur le ministère des Travaux publics et des Services gouvernementaux* (chaque partie étant un « client »). Bien que le Canada puisse étendre cette solution de logiciel-service à tout client de son choix, la présente demande de soumissions n'interdit pas au Canada d'avoir recours à une autre méthode d'approvisionnement pour les entités du gouvernement du Canada qui éprouvent le même besoin ou un besoin semblable.

- (3) Le besoin est assujéti aux dispositions de l'Accord sur les marchés publics de l'Organisation mondiale du commerce (AMP-OMC), de l'Accord de libre-échange nord-américain (ALENA), de l'Accord de libre-échange Canada-Pérou (ALECP), de l'Accord de libre-échange

Canada-Chili (ALECC), de l'Accord de libre-échange Canada-Colombie, de l'Accord de libre-échange Canada-Panama s'il est en vigueur et de l'Accord sur le commerce intérieur (ACI).

- (4) Une exigence du Programme de contrats fédéraux pour l'équité en matière d'emploi est associée au présent besoin; veuillez-vous reporter à la partie 5 – Attestations, à la partie 7 – Clauses du contrat subséquent, et au formulaire 4 intitulé « Programme de contrats fédéraux pour l'équité en matière d'emploi – Attestation ».
- (5) La présente demande de soumissions comporte des exigences en matière de sécurité. Pour de plus amples renseignements, consulter la partie 6 – Exigences relatives à la sécurité, exigences financières et autres exigences et la partie 7 – Clauses du contrat subséquent. Pour en savoir plus sur le filtrage de sécurité du personnel et de l'organisation ainsi que sur les clauses de sécurité, les soumissionnaires doivent consulter le site Web du Programme de sécurité des contrats de Travaux publics et Services gouvernementaux Canada.
- (6) Les soumissionnaires peuvent utiliser le service Connexion postal de la Société canadienne des postes pour présenter leur soumission par voie électronique. Les soumissionnaires doivent consulter la partie 2, Instructions à l'intention des soumissionnaires, et la partie 3, Instructions pour la préparation des soumissions, de la demande de soumissions pour obtenir de plus amples renseignements.

1.3 Comptes rendus

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

1.4 Conflit d'intérêts

- (1) Les soumissionnaires sont priés de se reporter aux dispositions relatives aux conflits d'intérêts du Guide des CCUA 2035, Conditions générales – besoins plus complexes de services (2018-06-21), publiées sur le site Web de TPSGC, à l'adresse suivante :

<https://achatsetventes.gc.ca/politiques-et-lignes-directrices/guide-des-clauses-et-conditions-uniformisees-d-achat>

- (2) Sans limiter d'aucune façon les dispositions décrites au paragraphe 1.4(a) ci-dessus, les soumissionnaires sont priés de noter que le Canada a fait appel aux ressources et aux entrepreneurs suivants du secteur privé, qui ont assuré la prestation de certains services, à savoir l'examen du contenu dans le cadre de la préparation de la présente DP. Ces personnes ont eu ou pourraient avoir accès aux renseignements relatifs au contenu de la DP ou à d'autres documents ayant trait à la demande de soumissions pour le SAGU :

Milos Simovic de :

Simke Consulting Inc.

75, promenade Meadowbreeze

Kanata (Ontario)

K2M 2L9

613-240-2716

- (3) Toute soumission reçue de l'un des entrepreneurs mentionnés ci-dessus, qu'il soit un soumissionnaire unique, une coentreprise ou le sous-traitant d'un soumissionnaire, ou toute soumission à laquelle l'une des ressources susmentionnées a contribué dans la soumission sera considérée comme étant en infraction aux dispositions relatives au conflit d'intérêts mentionnées au paragraphe 1.4 et sera déclarée non recevable.

PARTIE 2 – INSTRUCTIONS À L'INTENTION DES SOUMISSIONNAIRES

2.1 Instructions, clauses et conditions uniformisées

- (1) Toutes les instructions, clauses et conditions identifiées dans la demande de soumissions par un numéro, une date et un titre figurent dans le *Guide des clauses et conditions uniformisées d'achat* publié par Travaux publics et Services gouvernementaux Canada.
- (2) Les soumissionnaires qui présentent une soumission s'engagent à respecter les instructions, les clauses et les conditions de la demande de soumissions et acceptent les clauses et les conditions du contrat subséquent.
- (3) Les exigences des « Instructions uniformisées – biens ou services – besoins concurrentiels » [2003 \(2019-03-04\)](#), sont incorporées par renvoi dans la demande de soumissions et en font partie intégrante.
- (4) Le paragraphe 5.4 des « Instructions uniformisées – biens ou services – besoins concurrentiels » [2003](#), est modifié comme suit :
- Supprimer : 60 jours
Insérer : 250 jours

2.2 Présentation des soumissions

Pour les soumissionnaires qui choisissent d'utiliser Connexion postal pour la clôture des soumissions au Module de réception des soumissions de la région de la capitale nationale (RCN), l'adresse électronique est :

tpsgc.dgareceptiondessoumissions-abidreceiving.pwgsc@tpsgc-pwgsc.gc.ca

** Il est à noter qu'une adresse postale canadienne est nécessaire pour utiliser le service Connexion postal. Si le soumissionnaire n'en a pas, il peut utiliser l'adresse du Module de réception des soumissions indiquée dans la demande de soumissions pour s'inscrire au service Connexion postal.

Remarque : Les soumissions envoyées directement à cette adresse courriel ne seront pas acceptées. Cette adresse courriel doit être utilisée pour ouvrir une conversation Connexion postal, de la manière décrite dans les « Instructions uniformisées – biens ou services – besoins concurrentiels » [2003](#), ou pour envoyer des soumissions dans un message Connexion postal si le soumissionnaire utilise sa propre licence d'utilisateur pour Connexion postal.

2.3 Ancien fonctionnaire

- (1) Les contrats attribués à d'anciens fonctionnaires qui touchent une pension ou qui ont reçu un paiement forfaitaire doivent résister à l'examen scrupuleux du public et constituer une dépense équitable des fonds publics. Afin de respecter les politiques et les directives du Conseil du Trésor sur les contrats attribués à d'anciens fonctionnaires, les soumissionnaires doivent fournir les renseignements exigés ci-dessous avant l'attribution du contrat. Si la réponse aux questions et, s'il y a lieu, les renseignements requis n'ont pas été fournis à la date de la fin de l'évaluation des soumissions, le Canada informera le soumissionnaire du délai qui lui est imparti pour fournir l'information. Le défaut de répondre à la demande du Canada et de se conformer aux exigences dans les délais prévus aura pour conséquence de rendre la soumission non recevable.

(2) Définitions

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

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

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

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

(3) Ancien fonctionnaire touchant une pension

Selon les définitions fournies ci-dessus, le soumissionnaire est-il un ancien fonctionnaire touchant une pension? **Oui () Non ()**
Si oui, le soumissionnaire doit fournir l'information suivante pour tous les anciens fonctionnaires touchant une pension, le cas échéant :

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

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

(4) Directive sur le réaménagement des effectifs

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

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

- (a) le nom de l'ancien fonctionnaire;
- (b) les conditions de l'incitatif versé sous forme de paiement forfaitaire;
- (c) la date de la cessation d'emploi;
- (d) le montant du paiement forfaitaire;
- (e) le taux de rémunération qui a servi au calcul du paiement forfaitaire;
- (f) la période du paiement forfaitaire, y compris la date de début, la date de fin et le nombre de semaines;
- (g) le nombre et le montant (honoraires) des autres contrats assujettis aux conditions d'un programme de réaménagement des effectifs.

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

2.4 Demande de renseignements – Demande de soumissions

- (1) Toutes les demandes de renseignements doivent être présentées par écrit à l'autorité contractante au moins **10 jours civils** avant la date de clôture des soumissions. Les demandes de renseignements reçues après cette date pourraient rester sans réponse.
- (2) Les soumissionnaires doivent citer le plus fidèlement possible le numéro de l'article de la demande de soumissions auquel se rapporte leur demande de renseignements. Les soumissionnaires doivent prendre soin d'énoncer chaque question de façon suffisamment détaillée pour que le Canada puisse y répondre avec exactitude. Les demandes de renseignements techniques qui ont un caractère exclusif doivent porter clairement la mention « exclusif » vis-à-vis de chaque article pertinent. Les éléments portant la mention « exclusif » feront l'objet d'une discrétion absolue, sauf dans les cas où le Canada considère que la demande de renseignements n'a pas un caractère exclusif. Dans ce cas, le Canada peut réviser les questions ou encore demander au soumissionnaire de le faire, afin d'en éliminer le caractère exclusif et ainsi de permettre la transmission des réponses à tous les soumissionnaires. Le Canada pourrait ne pas répondre aux demandes de renseignements dont la formulation ne permettrait pas de les diffuser à tous les soumissionnaires.

2.5 Lois applicables

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

Remarque à l'intention des soumissionnaires : À leur discrétion, les soumissionnaires peuvent indiquer les lois applicables d'une province ou d'un territoire canadien de leur choix, sans que la validité de leur soumission soit mise en question, en supprimant le nom de la province ou du territoire canadien précisé et en insérant le nom de la province ou du territoire canadien de leur choix. Si aucun changement n'est indiqué, cela signifie que le soumissionnaire accepte les lois applicables précisées. *Les soumissionnaires doivent indiquer la province ou le territoire du Canada de leur choix dans le formulaire de présentation de la soumission.*

2.6 Améliorations apportées au besoin pendant la demande de soumissions

Les soumissionnaires qui estiment qu'ils peuvent améliorer, techniquement ou technologiquement, le devis descriptif ou l'énoncé des travaux contenus dans la demande de soumissions sont invités à fournir des suggestions par écrit à l'autorité contractante identifiée dans la demande de soumissions. Les soumissionnaires doivent indiquer de façon claire les améliorations proposées, ainsi que les motifs de celles-ci. Les suggestions, qui ne restreignent pas la concurrence ou qui ne favorisent pas un soumissionnaire en particulier, seront examinées à la condition d'être soumises à l'autorité contractante, conformément au paragraphe intitulé « Demandes de renseignements – en période de soumission ». Le Canada aura le droit d'accepter ou de rejeter n'importe laquelle ou la totalité des suggestions proposées.

2.7 Données volumétriques

Les données ont été fournies aux soumissionnaires afin de les aider à préparer leurs soumissions. L'inclusion de ces données dans la présente demande de soumissions ne représente pas un engagement par le Canada du fait que l'utilisation future du SAGU par le Canada correspondra à ces données. Elles sont fournies strictement à titre d'information.

PARTIE 3 – INSTRUCTIONS POUR LA PRÉPARATION DES SOUMISSIONS

3.1 Instructions pour la préparation des soumissions

- (1) Les soumissionnaires doivent présenter leur soumission par voie électronique. Le Canada demande au soumissionnaire de présenter sa soumission conformément à l'article 08 des instructions uniformisées de 2003. Le système Connexion postel a une limite de 1 Go par message individuel affiché et de 20 Go par conversation.

- (2) Le soumissionnaire doit présenter les sections suivantes de sa soumission dans un (1) fichier PDF :

- (a) Section I : Soumission technique
- (b) Section II : Soumission financière
- (c) Section III : Certifications
- (d) Section IV : Information sur l'intégrité de la chaîne d'approvisionnement

3.2 Présentation d'une seule soumission

- (1) Un soumissionnaire et les entités qui y sont liées ne peuvent soumettre qu'une seule soumission en réponse à la présente demande de soumissions. Si un soumissionnaire ou une entité liée participe à plus d'une soumission (participer signifie faire partie du groupe soumissionnaire, et non pas être un sous-traitant), le Canada donnera deux jours ouvrables à ces soumissionnaires pour indiquer laquelle des soumissions devra être prise en compte par le Canada. À défaut de respecter ce délai, les soumissions visées seront rejetées.

- (2) Aux fins du présent article, peu importe la province ou le territoire où les entités ont été constituées en société ou formées juridiquement (qu'il s'agisse d'une personne physique, d'une société, d'un partenariat, etc.), une entité est considérée comme étant « liée » à un soumissionnaire :

- (a) S'il s'agit de la même personne morale (c'est-à-dire la même personne physique, société, société de personnes, société à responsabilité limitée, etc.);
- (b) s'il s'agit de « personnes liées » ou de « personnes affiliées » au sens de la *Loi de l'impôt sur le revenu du Canada*;
- (c) Si les entités entretiennent une relation fiduciaire (découlant d'un arrangement entre agences ou toute autre forme de relation fiduciaire) ou ont entretenu une telle relation au cours des deux années précédant la date de clôture des soumissions;
- (d) Si les entités ne sont pas dépendantes l'une de l'autre ou d'un même tiers;
- (e) Si les membres individuels d'une coentreprise ne peuvent pas participer à une autre soumission en présentant eux-mêmes une soumission ou en participant à une autre coentreprise.

(3) Expérience de la coentreprise

- (a) Si le soumissionnaire est une coentreprise qui possède de l'expérience à ce titre, il peut citer l'expérience qu'il a acquise en tant que coentreprise.

Exemple : Supposons que le soumissionnaire est une coentreprise constituée des membres L et O, et que la demande de soumissions exige que le soumissionnaire ait de l'expérience dans la prestation de services d'entretien et de services de dépannage à un client comptant au moins 10 000 utilisateurs, pendant 24 mois. L'entrepreneur, c'est-à-dire la coentreprise

constituée des membres L et O, a déjà fourni ces services par le passé. Le soumissionnaire peut citer cette expérience pour répondre à l'exigence. Si le membre L a acquis cette expérience alors qu'il était en coentreprise avec une tierce partie, N, cette expérience ne peut pas être utilisée parce que N ne fait pas partie de la coentreprise qui présente une soumission.

- (b) Une coentreprise peut se fonder sur l'expérience de l'un de ses membres pour satisfaire à tout critère technique de la présente demande de soumissions.

Exemple : Supposons que le soumissionnaire est une société en participation constituée des membres X, Y et Z, et que la demande de soumissions exige a) que le soumissionnaire ait trois années d'expérience dans la prestation de services d'entretien et b) qu'il en ait deux dans l'intégration de matériel informatique à des réseaux complexes. Chacune de ces deux exigences peut alors être satisfaite par un membre différent de ladite coentreprise. Cependant, pour un critère donné, par exemple celui qui concerne l'expérience de trois ans dans la prestation de services de maintenance, le soumissionnaire ne peut pas indiquer que chaque membre, soit X, Y et Z, a un an d'expérience pour un total de trois ans. Cette proposition serait considérée comme irrecevable.

- (c) Les membres de la coentreprise ne peuvent pas combiner leurs compétences avec celles d'autres membres de coentreprise pour satisfaire à un seul critère technique de la présente demande de soumissions. Toutefois, un membre de la coentreprise peut ajouter à son expérience individuelle celle de la coentreprise elle-même. Chaque fois qu'il doit faire la preuve qu'il répond à un critère, le soumissionnaire doit indiquer quel membre de la coentreprise y répond. Si le soumissionnaire n'a pas précisé le membre de la coentreprise qui satisfait à l'exigence, l'autorité contractante lui donnera l'occasion de soumettre les renseignements pendant la période d'évaluation. Si le soumissionnaire ne fournit ce renseignement pendant la période fixée par l'autorité contractante, sa soumission sera déclarée non recevable.

Exemple : Supposons que le soumissionnaire est une coentreprise constituée des membres A et B, et que la demande de soumissions exige que le soumissionnaire ait déjà fourni des ressources durant 100 jours facturables, au minimum. Le soumissionnaire peut montrer qu'il possède l'expérience requise en soumettant :

- a. Les contrats signés par A;
- b. Les contrats signés par le membre B; ou
- c. Les contrats signés par les membres A et B en coentreprise; ou
- d. Les contrats signés par A et les contrats signés par A et B en coentreprise; ou
- e. Les contrats signés par B et les contrats signés par A et B en coentreprise;

Le tout totalise 100 jours ouvrables.

- (d) Les soumissionnaires qui ont des questions concernant l'évaluation des soumissions présentées par une coentreprise devraient poser leurs questions dans le cadre du processus de demande de renseignements dès que possible durant la période de demande de soumissions.

3.3 Section I : Soumission technique

- (1) Dans leur soumission technique, les soumissionnaires devraient démontrer leur compréhension des exigences contenues dans la demande de soumissions et expliquer comment ils répondront à ces exigences. Les soumissionnaires doivent démontrer leur capacité et décrire l'approche qu'ils prendront de façon complète, concise et claire pour effectuer les travaux.

- (2) La soumission technique devrait aborder clairement et de manière suffisamment approfondie les points faisant l'objet des critères d'évaluation en fonction desquels la soumission sera évaluée. Il ne suffit pas de reprendre simplement les énoncés contenus dans la demande de soumissions. Afin de faciliter l'évaluation de la soumission, le Canada demande que les soumissionnaires reprennent les sujets dans l'ordre des critères d'évaluation, sous les mêmes rubriques. Pour éviter les recoupements, les soumissionnaires peuvent faire référence à différentes sections de leur soumission en indiquant le numéro de l'alinéa et de la page où le sujet visé est déjà traité.
- (3) La soumission technique comprend les éléments suivants :
- (a) **Justification de la conformité technique** : La soumission technique doit prouver que le SAGU proposé par le soumissionnaire est conforme aux paragraphes de l'annexe A – Énoncé des besoins.
 - (b) Le soumissionnaire doit fournir une description de ses services de soutien et de maintenance, qui doivent être conformes aux exigences décrites dans la partie Clauses du contrat subséquent ainsi que dans l'Énoncé des besoins. Au minimum, le soumissionnaire doit décrire :
 - a. Ses procédures d'intervention et de résolution de problèmes;
 - b. Ses procédures d'acheminement au palier approprié;
 - c. Le soutien offert;
 - d. Toute amélioration aux fonctionnalités de base proposée par le soumissionnaire.

(c) **Documentation technique** : Le soumissionnaire doit fournir les documents techniques, comme les manuels de l'utilisateur, les captures d'écran, les documents de conception ou de gestion du système (ou d'autres sources d'information), à l'appui de la réponse du soumissionnaire à chaque exigence (une copie électronique des documents techniques à l'appui de la soumission technique est acceptable). L'indication de liens vers des sites Web n'est pas acceptable, et dans le cas où une telle indication sert à confirmer une exigence obligatoire, la soumission sera considérée comme non recevable. Le soumissionnaire devrait indiquer l'endroit exact où figure le document de référence, y compris le titre du document, la page et le numéro d'article. Tout document de référence indiqué par le soumissionnaire pour attester la conformité doit accompagner la soumission (copie papier ou électronique). Un document qui n'est pas joint à la soumission ne sera pas pris en considération par le Canada. Lorsque la référence n'est pas suffisamment précise, le Canada peut demander que le soumissionnaire dirige le Canada vers l'endroit approprié dans le document.

(d) **Accords sur les niveaux de service** : Les entrepreneurs doivent présenter leurs accords de niveau de service (ANS) publiés, dans l'annexe F – Accords sur les niveaux de service (ANS) de la solution de logiciel-service.

En présentant une soumission, l'entrepreneur reconnaît et accepte que toutes les conditions contenues dans l'annexe F - Accords de niveau de service de solution ANS qui visent à interpréter le contrat, sont le même objet ou un objet similaire, ou sont liées aux conditions contenues dans les clauses du contrat, sont considérés comme frappés et sont sans effet.

Les engagements relatifs au niveau de service (décrits dans les accords sur les niveaux de service) doivent inclure un soutien aux clients commerciaux qui prévoit, au moins, un soutien publié et disponible sur le marché (garantie, maintenance et services de soutien) habituellement fourni aux clients qui fournissent une solution de logiciel-service.

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

- a. Période durant laquelle le soumissionnaire offrira du soutien au client;
- b. Coordonnées et renseignements concernant la procédure pour obtenir du soutien;
- c. Procédures de résolution de problèmes;
- d. Délais de réponse;
- e. Procédures relatives au traitement (quand et comment) des communications par téléphone ou par courriel;
- f. Disponibilité du site Web de soutien pour les utilisateurs du Canada (p. ex., jour et nuit, 365 jours par an, 99,9 % du temps).
- g. Services de maintenance (p. ex., correctifs, mises à jour, versions majeures ou mineures)

3.4 Section II : Soumission financière

- (1) **Prix** : Les soumissionnaires doivent présenter leur soumission financière conformément à l'annexe B – Tableau des prix, sans condition, hypothèse, ni restriction. Toute proposition financière qui prétend restreindre la façon dont le Canada acquiert des biens ou des services dans le cadre d'un contrat subéquente, à l'exception des limitations établies clairement dans cette demande de soumissions, sera considérée comme irrecevable. Le montant total de la taxe sur les produits et services ou de la taxe de vente harmonisée doit être indiqué séparément, s'il y a lieu. Sauf indication contraire, les soumissionnaires doivent inclure un seul prix ferme, tout compris, en dollars canadiens, dans chaque cellule des tableaux où il faut saisir des données.
- (2) **Coûts à indiquer** : La soumission financière doit indiquer tous les coûts relatifs au besoin décrit dans la demande de soumissions pour toute la durée du contrat, y compris les années d'option. Il incombe entièrement au soumissionnaire d'indiquer tout le matériel, les logiciels, les périphériques, le câblage et les composants nécessaires pour satisfaire aux exigences de la présente demande de soumissions, ainsi que les prix de ces articles.
- (3) **Prix non indiqués** : On demande aux soumissionnaires d'indiquer « 0,00 \$ » pour tout article qu'ils ne comptent pas facturer ou qui fait déjà partie d'autres prix présentés dans les tableaux. Si le soumissionnaire laisse en blanc un espace réservé à un prix, le gouvernement du Canada donne à ce prix la valeur de « 0,00 \$ » aux fins de l'évaluation et il peut demander au soumissionnaire de confirmer que le prix est bien de 0,00 \$. Aucun soumissionnaire ne sera autorisé à ajouter ou à modifier un prix lors de cette confirmation. Si le soumissionnaire refuse de confirmer que le prix d'un champ vierge est de 0,00 \$, sa soumission sera déclarée irrecevable.

3.5 Section III : Certifications

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

3.6 Section IV : Exigences d'intégrité de la chaîne d'approvisionnement

- (1) Les soumissionnaires doivent satisfaire aux exigences d'intégrité de la chaîne d'approvisionnement (ICA) décrites à l'annexe A – Énoncé des besoins, O10 et O11, de la DP.
- (2) Les soumissionnaires doivent présenter l'information sur la sécurité de la chaîne d'approvisionnement (ISCA), décrite dans l'annexe F – Modèle de présentation de l'ICA, et doivent tenir ou mettre à jour toute information sur l'ISCA comme requis par l'autorité de sécurité de la chaîne d'approvisionnement. Le Canada utilisera l'ICA pour vérifier si, à son avis, la chaîne d'approvisionnement du soumissionnaire peut faire en sorte que la solution de logiciel-service qu'il propose compromet ou sert à compromettre l'intégrité de la sécurité du matériel, des micrologiciels, des logiciels, des systèmes ou des renseignements lui appartenant, conformément au processus d'ICA décrit au paragraphe 4.4, **Processus d'intégrité de la chaîne d'approvisionnement**.

- (3) En présentant son ISCA, et compte tenu de la possibilité de participer à ce processus d'approvisionnement, le soumissionnaire accepte les modalités de l'accord de non-divulgaration qui figurent à l'annexe H, Accord de non-divulgaration lié à l'intégrité de la chaîne d'approvisionnement.

PARTIE 4 – PROCÉDURES D'ÉVALUATION ET MÉTHODE DE SÉLECTION

4.1 Procédures d'évaluation

- (1) Les soumissions seront évaluées par rapport à l'ensemble des exigences de la demande de soumissions, incluant les critères d'évaluation techniques et financiers. La procédure d'évaluation comporte plusieurs étapes, décrites ci-après. Même si l'évaluation et la sélection seront effectuées par étape, le fait que le Canada soit passé à une étape ultérieure ne signifie pas que ce dernier a irréfutablement déterminé que le soumissionnaire a réussi toutes les étapes précédentes. Le Canada se réserve le droit d'exécuter parallèlement certaines étapes de l'évaluation.
- (2) Une équipe composée de représentants du client et de TPSGC évaluera les soumissions pour le compte du Canada. Le Canada peut faire appel à des experts-conseils ou aux ressources du gouvernement pour évaluer les soumissions. Chaque membre de l'équipe chargée de l'évaluation ne participera pas nécessairement à tous les aspects de l'évaluation.
- (3) En plus de tout autre délai prescrit dans la demande de soumissions :
- (a) **Demandes de précisions** : Si le Canada demande des précisions au soumissionnaire quant à son offre ou s'il veut vérifier celle-ci, le soumissionnaire disposera d'un délai de trois jours ouvrables (ou d'un délai plus long précisé par écrit par l'autorité contractante) pour fournir les renseignements nécessaires au Canada. À défaut de respecter ce délai, la soumission sera jugée non recevable.
- a. **Demande de renseignements supplémentaires** : Si le Canada demande d'autres renseignements pour l'une des raisons qui suivent, selon la section intitulée « Déroulement de l'évaluation » du document 2003, *Instructions uniformisées – biens ou services – besoins concurrentiels* : vérifier une partie ou l'ensemble des renseignements fournis par le soumissionnaire dans sa soumission;
- b. Communiquer avec une ou plusieurs des références citées par le soumissionnaire (p. ex., les références citées dans les curriculum vitae des ressources individuelles) dans le but de confirmer les renseignements fournis par le soumissionnaire;
- c. Le soumissionnaire doit soumettre les renseignements demandés par le Canada dans les 3 jours ouvrables suivant la demande de l'autorité contractante.
- (b) Prolongation de délai : L'autorité contractante se réserve le droit d'accepter ou de refuser les demandes de prolongation de délai présentées par le soumissionnaire.

4.2 Évaluation technique

- (1) Exigences obligatoires :

- (a) On examinera chaque soumission pour s'assurer qu'elle respecte toutes les exigences obligatoires de la demande de soumissions. Tous les éléments de la demande de soumissions qui constituent des exigences obligatoires sont désignés précisément par les termes « doit », « doivent » ou « obligatoire ». Les soumissions qui ne respectent pas l'ensemble des exigences obligatoires seront déclarées non recevables et rejetées.
- (b) Les exigences obligatoires sont décrites à l'annexe A – Énoncé des besoins.

(2) Exigences cotées :

- (a) Chaque soumission sera cotée par l'attribution d'une note aux exigences cotées, qui sont précisées dans la demande de soumissions par le terme « cotées » ou au moyen d'un renvoi à une note. Les soumissions incomplètes et ne contenant pas tous les renseignements exigés dans la demande de soumissions seront cotées en conséquence.
- (b) Les exigences cotées sont décrites à l'annexe A, Énoncé des besoins.

4.3 Évaluation financière

- (1) L'évaluation financière sera effectuée en calculant le **montant total de la soumission** à l'aide des tableaux de prix remplis par les soumissionnaires.
- (2) Le processus utilisé pour l'évaluation financière est décrit à l'annexe B – Base de paiement.

(3) Formules des tableaux de prix

Si les tableaux de prix fournis aux soumissionnaires ne comprennent aucune formule, le Canada peut entrer les prix fournis par les soumissionnaires dans un nouveau tableau, s'il estime que la formule ne fonctionne plus correctement selon la version fournie par le soumissionnaire.

(4) Justification des taux des services professionnels

Selon l'expérience du Canada, les soumissionnaires proposent de temps à autre des taux au moment de déposer une soumission pour une ou plusieurs catégories de personnel qu'ils refusent de respecter par la suite, parce que ces taux ne leur permettent pas de recouvrer leurs propres coûts ou de réaliser un profit. Dans le cadre de l'évaluation des taux des services professionnels présentés dans la soumission, le Canada peut, sans toutefois y être obligé, demander une justification des taux, conformément au présent article. Si le Canada demande une justification de prix, elle sera demandée à tous les soumissionnaires conformes proposant un tarif au moins 20 % inférieur au à la médiane des tarifs offerts par tous les soumissionnaires conformes pour la ou les mêmes catégories de ressources. Si le Canada demande une justification des prix, le soumissionnaire doit fournir les renseignements suivants :

- (a) une facture (ainsi que le numéro de série du contrat ou tout autre élément permettant d'identifier le contrat) indiquant que le soumissionnaire a offert et facturé des services similaires à ceux qui seraient fournis par cette catégorie de ressource à un client (qui n'a aucun lien de dépendance avec le soumissionnaire) dans la catégorie de ressources pertinente, services qui ont été offerts pour une période d'au moins trois mois au cours des douze mois précédant la date de clôture de la demande de soumissions, et que les services ont été rendus à un taux quotidien égal ou inférieur à celui proposé au Canada;
- (b) relativement à la facture mentionnée en (i), une preuve du client du soumissionnaire démontrant que les services indiqués sur la facture comprennent au minimum 50 % des tâches énumérées dans l'énoncé des travaux pour la catégorie de ressources évaluée, et ce, à un taux déraisonnablement bas. Il peut s'agir d'une copie du contrat (dans lequel on décrit les services à offrir et où l'on démontre qu'au moins 50 % des tâches sont les mêmes que celles qui doivent être effectuées dans le cadre de l'énoncé des travaux de la présente demande de soumissions) ou d'une attestation signée du client indiquant que les services

notés sur la facture comprendraient au moins 50 % des tâches qui doivent être effectuées en vertu de l'énoncé des travaux de la présente demande de soumissions;

- (c) pour chacun des contrats pour lesquels une facture est présentée à titre de justification, le curriculum vitae de la ressource qui a offert les services dans le cadre de ce contrat afin de démontrer que la ressource répondrait aux exigences obligatoires et obtiendrait la note de passage pour tous les critères cotés de la catégorie de ressources faisant l'objet d'une justification des taux;
- (d) le nom, le numéro de téléphone et, si possible, l'adresse de courriel d'une personne-ressource du client ayant reçu chacune des factures présentées au point (i), afin que le Canada puisse valider tout renseignement fourni par le soumissionnaire.

- (5) Lorsque le Canada demande une justification des taux offerts pour une catégorie de ressources donnée, il incombe entièrement au soumissionnaire de présenter l'information (décrite ci-dessus, ou d'autres renseignements pouvant être demandés par le Canada, y compris les renseignements qui permettraient au Canada de vérifier l'information auprès de la ressource proposée) qui permettra au Canada de déterminer s'il peut compter en toute confiance sur la capacité du soumissionnaire à fournir les services requis aux taux indiqués dans la soumission. Lorsque le Canada détermine que l'information fournie par le soumissionnaire ne justifie pas des taux déraisonnablement bas, la proposition sera jugée irrecevable.

4.4 Processus d'intégrité de la chaîne d'approvisionnement

- (1) Au cours du processus d'appel d'offres, de la période du contrat et de toute période d'option subséquente, l'autorité responsable de la sécurité de la chaîne d'approvisionnement désignée par le Canada peut, en fonction de son mandat de sécurité nationale visant à protéger l'infrastructure de TI du Canada ainsi qu'à évaluer les menaces, les risques et les points vulnérables, évaluer l'ISCA du soumissionnaire.
- (2) Le Canada évaluera si, à son avis, la chaîne d'approvisionnement du soumissionnaire pourrait faire en sorte que la solution proposée compromette ou serve à compromettre l'intégrité de la sécurité du matériel, des micrologiciels, des logiciels, des systèmes ou des renseignements lui appartenant ou représenter une menace à la sécurité nationale, conformément à la section 2 de l'annexe D, Processus d'intégrité de la chaîne d'approvisionnement.
- (3) Il s'agit d'une condition préalable à l'attribution d'un contrat qu'un soumissionnaire satisfasse à l'évaluation de l'intégrité de la chaîne d'approvisionnement de l'autorité de sécurité. Le Canada évaluera si, à son avis, la chaîne d'approvisionnement du soumissionnaire pourrait faire en sorte que la solution proposée compromette ou serve à compromettre l'intégrité de la sécurité du matériel, des micrologiciels, des logiciels, des systèmes ou des renseignements lui appartenant, conformément à la section 4 de l'annexe D, Processus d'intégrité de la chaîne d'approvisionnement.

4.5 Méthode de sélection

- (1) Pour être déclarée recevable, une soumission doit :
 - (a) respecter toutes les conditions de la demande de soumissions;
 - (b) satisfaire à toutes les exigences de la demande de soumissions;
 - (c) satisfaire à tous les critères d'évaluation techniques obligatoires;

- (d) obtenir une note d'au moins 75 % des exigences cotées.

Les soumissions qui ne respectent pas les critères i), ii), iii) ou iv) seront jugées irrecevables.

- (2) Le prix reçoit une valeur de cotation qui est prise en compte dans le calcul de la note totale de la soumission. Soixante-dix pour cent des points seront accordés pour la soumission technique, et trente pour cent des points seront accordés pour la soumission financière.

Pour effectuer ce calcul, on utilise la formule suivante :

$$\left(\frac{\text{Note pour les exigences cotées de la soumission}}{\text{Note maximale possible}} \right) \times 70 \% = \text{Total 1}$$

$$\left(\frac{\text{Prix total évalué le plus bas}}{\text{Prix total évalué de la soumission}} \right) \times 30 \% = \text{Total 2}$$

(Total 1) + (Total 2) = Meilleure cote combinée de mérite technique et de prix

- (3) La soumission conforme qui sera classée au premier rang sera celle qui satisfait à tous les critères obligatoires, qui satisfait ou dépasse toutes les notes minimales requises pour les exigences cotées et qui offre la **meilleure cote combinée à la suite de l'évaluation du prix et du mérite technique**, calculée selon la formule ci-dessus. La soumission recevable la mieux cotée sera recommandée pour l'attribution du contrat.

- (4) Les soumissionnaires devraient noter que l'attribution des marchés reste assujettie à la procédure interne d'approbation du Canada, qui prévoit l'approbation obligatoire du financement selon le montant de tout marché proposé. Même si on a recommandé l'attribution du contrat à un soumissionnaire, un marché ne sera préparé que si l'approbation interne est obtenue conformément aux politiques internes du Canada. Si l'approbation n'est pas obtenue, aucun marché ne sera attribué.

- (5) Si plus d'un soumissionnaire est classé au premier rang parce que les notes globales sont identiques, le soumissionnaire ayant la meilleure note relative au prix se verra accorder le premier rang.

4.6 Contrôle de validation de la soumission classée au premier rang

- (1) Dans le cadre d'un contrôle de validation de la soumission, le Canada pourra examiner la solution proposée dans la soumission classée au premier rang (établie après l'évaluation financière) afin de confirmer qu'elle fonctionnera comme indiqué dans la soumission et qu'elle satisfait aux exigences de fonctionnalité technique énoncées dans l'annexe A. Le contrôle de validation de la soumission aura lieu dans un établissement de la région de la capitale nationale, prévu par le Canada, qui simule l'environnement technique requis, tel qu'il est décrit dans l'annexe A, des besoins.

- (2) Après avoir été informé par l'autorité contractante, le soumissionnaire aura au plus cinq jours ouvrables pour préparer la solution logicielle proposée. Le Canada effectuera alors le contrôle de validation. Jusqu'à deux représentants du soumissionnaire peuvent être présents pendant le contrôle de validation de la soumission. Le ou les représentants nommés dans la soumission pour la prestation du soutien technique doivent être disponibles en personne ou par téléphone pour donner des conseils techniques et des explications pendant le contrôle de validation de la soumission; toutefois, si un représentant n'est pas disponible, le Canada n'est pas obligé de retarder le contrôle de validation de la soumission.

(3) Le Canada consignera les résultats du contrôle de validation de la soumission. Si le Canada détermine que la solution proposée ne satisfait pas à une exigence obligatoire de la demande de soumissions, la soumission ne passera pas le contrôle de validation de la soumission et sera rejetée. À la suite du contrôle de validation de la soumission, le Canada peut réduire la note accordée au soumissionnaire pour toute exigence cotée si ce contrôle ne valide pas la note attribuée au soumissionnaire en fonction de sa soumission écrite. La note du soumissionnaire ne sera pas augmentée à la suite d'un contrôle de validation de la soumission. S'il réduit la note du soumissionnaire à la suite du contrôle de validation, le Canada procédera à un nouveau classement des soumissionnaires.

(4) Dans le cadre du contrôle de validation, le soumissionnaire permet au Canada d'accéder à la solution qu'il propose, et ce, aux fins d'essai et d'évaluation.

4.7 Évaluation informatique du meilleur soumissionnaire

Avant l'attribution du contrat, le soumissionnaire retenu doit compléter le programme d'évaluation informatique du Centre canadien de Cybersécurité (CCCS)

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

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

PARTIE 5 – ATTESTATIONS ET RENSEIGNEMENTS SUPPLÉMENTAIRES

Pour qu'un contrat leur soit attribué, les soumissionnaires doivent fournir les attestations exigées et d'autres renseignements.

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

L'autorité contractante aura le droit de demander des renseignements supplémentaires pour vérifier les attestations du soumissionnaire. Le non-respect de toute demande ou exigence imposée par l'autorité contractante peut rendre la soumission non recevable ou constituer un manquement au contrat.

5.1 Attestations à joindre à la soumission

Les soumissionnaires doivent fournir les attestations ci-dessous dûment remplies avec leur soumission.

(1) Dispositions relatives à l'intégrité – Déclaration de condamnation à une infraction

Conformément aux dispositions relatives à l'intégrité des Instructions générales, tous les soumissionnaires doivent fournir avec leur proposition, **s'il y a lieu**, le formulaire de déclaration d'intégrité se trouvant sur le site Web des [formulaires de déclaration – Intégrité](#), afin que leur soumission soit prise en compte dans le cadre du processus d'approvisionnement.

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

Les attestations et les renseignements supplémentaires énumérés ci-dessous devraient être fournis avec la soumission, mais ils peuvent être fournis plus tard. Si l'une des attestations exigées ou l'un des renseignements supplémentaires requis n'est pas fourni conformément aux exigences, l'autorité contractante informera le soumissionnaire du délai dont il dispose pour le faire. Si le soumissionnaire ne fournit pas les attestations et les renseignements supplémentaires énumérés ci-dessous dans le délai établi, sa soumission sera déclarée non recevable.

(1) Dispositions relatives à l'intégrité – Documents exigés

Conformément à la section intitulée « Renseignements à fournir lors d'une soumission, de la passation d'un contrat ou de la conclusion d'un accord immobilier » de la [Politique d'inadmissibilité et de suspension](#), le soumissionnaire doit fournir la documentation requise, selon le cas, pour que son offre passe à l'étape suivante du processus.

(2) Programme de contrats fédéraux pour l'équité en matière d'emploi – Attestation de soumission

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

Le Canada aura le droit de déclarer une soumission non recevable si le soumissionnaire, ou tout membre de la coentreprise si le soumissionnaire est une coentreprise, figure sur la « Liste des soumissionnaires à admissibilité limitée du PCF » pour l'équité en matière d'emploi au moment de l'attribution du contrat.

Le Canada aura aussi le droit de résilier le contrat pour manquement si le soumissionnaire, ou tout membre de la coentreprise si le soumissionnaire est une coentreprise, figure sur la « [Liste d'admissibilité limitée à soumissionner au PCF](#) » pendant la durée du contrat.

Le soumissionnaire doit fournir à l'autorité contractante l'annexe G, Programme de contrats fédéraux pour l'équité en matière d'emploi – Attestation, dûment remplie avant l'attribution du marché. Si le soumissionnaire est une coentreprise, il doit fournir à l'autorité contractante

l'annexe J, Programme de contrats fédéraux pour l'équité en matière d'emploi – Attestation, dûment remplie pour chaque membre de la coentreprise.

PARTIE 6 – SÉCURITÉ, EXIGENCES FINANCIÈRES ET AUTRES EXIGENCES

6.1 Capacité financière

- 6.1.1 **Exigences en matière de capacité financière** : Le soumissionnaire doit avoir la capacité financière nécessaire pour répondre à ce besoin. Afin d'évaluer la capacité financière du soumissionnaire, l'autorité contractante pourra, dans un avis écrit à l'intention du soumissionnaire, exiger que ce dernier fournisse une partie ou la totalité des renseignements financiers dont il est question ci-dessous durant l'évaluation des soumissions. Le soumissionnaire doit fournir à l'autorité contractante les renseignements suivants dans un délai de quinze (15) jours ouvrables suivant la réception d'une demande de l'autorité contractante ou dans un délai précisé par l'autorité contractante dans l'avis.

- 6.1.1.1 Les états financiers vérifiés ou, si ces derniers ne sont pas disponibles, les états financiers non vérifiés (préparés par la firme de comptabilité externe du soumissionnaire, s'il y a lieu, ou encore préparés à l'interne si aucun état financier n'a été préparé par un tiers) pour les trois derniers exercices financiers du soumissionnaire ou, si l'entreprise est en opérations depuis moins de trois ans, pour toute la période en question (incluant au minimum le bilan, l'état des bénéfices non répartis, l'état des résultats et les notes afférentes aux états financiers).
- 6.1.1.2 Si les états financiers mentionnés au paragraphe 1.a) datent de plus de cinq mois précédant la date à laquelle l'autorité contractante demande l'information, le soumissionnaire doit également fournir, à moins que ce soit interdit par une loi dans le cas des sociétés ouvertes au public, les derniers états financiers trimestriels (comprenant un bilan et un état des résultats depuis le début de l'exercice), datant de deux mois précédant la date à laquelle l'autorité contractante demande cette information.
- 6.1.1.3 Si le soumissionnaire n'exerce pas ses activités depuis au moins un exercice complet, il doit fournir les renseignements suivants :
- i. le bilan d'ouverture en date de début des activités (dans le cas d'une corporation, un bilan à la date de la constitution de la société);
 - ii. les derniers états financiers trimestriels (comprenant un bilan et un état des résultats depuis le début de l'exercice) datant de deux mois précédant la date à laquelle l'autorité contractante demande cette information.
- 6.1.1.4 Une attestation de la part du directeur financier ou d'un signataire autorisé du soumissionnaire stipulant que les renseignements financiers fournis sont exacts et complets.
- 6.1.1.5 Une lettre de confirmation émise par toutes les institutions financières ayant fourni du financement à court terme au soumissionnaire. Cette lettre doit faire état du montant total des marges de crédit accordées au soumissionnaire ainsi que du crédit toujours disponible, et non utilisé, un mois précédant la date à laquelle l'autorité contractante demande cette information.

- 6.1.1.6 Un état mensuel détaillé des flux de trésorerie portant sur toutes les activités du soumissionnaire (y compris le besoin) pour les deux premières années du besoin visé par la demande de soumissions, à moins que ce soit interdit par une loi. Cet état doit contenir des détails sur les principales sources de financement et sur le montant de ce financement du soumissionnaire, ainsi que sur les principaux décaissements réalisés chaque mois, dans le cadre de toutes les activités du soumissionnaire. Toutes les hypothèses devraient y être expliquées, ainsi que toute information sur le mode de financement des déficits.
- 6.1.1.7 Un état mensuel détaillé des flux de trésorerie pour les deux premières années du besoin visé par la demande de soumissions, à moins que ce soit interdit par une loi. Cet état doit contenir des détails sur les principales sources de financement et sur le montant de ce financement du soumissionnaire, ainsi que sur les principaux décaissements réalisés chaque mois dans le cadre du besoin. Toutes les hypothèses devraient y être expliquées, ainsi que toute information sur le mode de financement des déficits.
- 6.1.2 Si le soumissionnaire est une coentreprise, les renseignements financiers exigés par l'autorité contractante doivent être fournis par chaque membre de la coentreprise.
- 6.1.3 Si le soumissionnaire est une filiale d'une autre entreprise, alors les renseignements financiers mentionnés aux paragraphes 1. a) à f) exigés par l'autorité contractante doivent être fournis par la société mère elle-même. Toutefois, la fourniture des renseignements financiers de la société mère ne répond pas à elle seule à l'exigence selon laquelle le soumissionnaire doit fournir ses renseignements financiers, et la capacité financière de la société mère ne peut pas remplacer la capacité financière du soumissionnaire, à moins qu'un consentement de la société mère à signer une garantie de la société mère, rédigée par Travaux publics et Services gouvernementaux Canada (TPSGC), ne soit fourni avec les renseignements exigés.
- 6.1.4 Renseignements financiers déjà fournis à TPSGC: Le soumissionnaire n'est pas tenu de soumettre de nouveau des renseignements financiers demandés par l'autorité contractante qui sont déjà détenus en dossier à TPSGC par la Direction des services des politiques, de la vérification et de l'analyse des coûts du Secteur de la politique, du risque, de l'intégrité et de la gestion stratégique, à condition que dans le délai susmentionné :
- 6.1.4.1 le soumissionnaire indique par écrit à l'autorité contractante les renseignements précis qui sont en dossier et le besoin à l'égard duquel ces renseignements ont été fournis;
- 6.1.4.2 le soumissionnaire autorise l'utilisation de ces renseignements pour ce besoin.
- Il incombe au soumissionnaire de confirmer auprès de l'autorité contractante que ces renseignements sont encore détenus par TPSGC.

6.1.5 **Autres renseignements** : Le Canada se réserve le droit de demander au soumissionnaire de fournir tout autre renseignement requis par le Canada pour procéder à une évaluation complète de la capacité financière du soumissionnaire.

6.1.6 **Confidentialité** : Si le soumissionnaire fournit au Canada, à titre confidentiel, les renseignements exigés ci-dessus et l'informe de la confidentialité des renseignements divulgués, le Canada doit traiter ces renseignements de façon confidentielle, suivant les dispositions de la Loi sur l'accès à l'information, L.R., 1985, ch. A-1, alinéas 20(1)b) et c).

6.1.7 **Sécurité** : Pour déterminer si le soumissionnaire a la capacité financière requise pour répondre au besoin, le Canada pourra prendre en considération toute garantie que le soumissionnaire peut lui offrir, aux frais du soumissionnaire (par exemple, une lettre de crédit irrévocable provenant d'une institution financière enregistrée et émise au nom du Canada, une garantie d'exécution provenant d'une tierce partie, ou toute autre forme de garantie exigée par le Canada).

6.2 Exigences liées au Programme de sécurité industrielle concernant les informations en nuage « Protégé B »

a) Généralités

i) *L'objectif* : L'objectif de cette annexe est d'énoncer les obligations de l'entrepreneur relativement à la bonne gestion des données du Canada, incluant la protection contre la modification non autorisée, à l'accès ou l'exfiltration, conformément à l'entente, à la présente annexe et aux mesures de sécurité de l'entrepreneur (collectivement, les « **obligations en matière de sécurité** »).

ii) *Transmission des obligations en matière de sécurité* : Les obligations de l'entrepreneur contenues dans les présentes obligations en matière de sécurité doivent être transmises par l'entrepreneur à tous les sous-traitants dans la mesure applicable.

iii) *Gestion du changement* :

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

(B) L'entrepreneur doit informer le Canada de tous les changements qui pourraient avoir une incidence négative sur la solution, y compris les améliorations ou changements de nature technologique, administrative ou autre.

(C) L'entrepreneur convient d'offrir toutes les améliorations disponibles sur le marché dans le cadre de son offre de services standard, sans frais supplémentaires pour le Canada.

b) Attestations

Les parties reconnaissent les points suivants :

i) Les données du Canada sont visées par les présentes obligations en matière de sécurité.

ii) Nonobstant toute autre disposition de la présente annexe, les parties ont la responsabilité partagée d'élaborer et de tenir à jour des politiques, des procédures et des contrôles de sécurité relatifs aux données du Canada.

iii) L'entrepreneur ne doit pas avoir obtenu ou tenté d'obtenir la garde des données du Canada, ni d'avoir permis à tout membre du personnel des services nuage d'accéder aux données du Canada avant la mise en œuvre des exigences de sécurité énoncées dans la présente annexe, à la date de l'attribution du contrat ou avant cette date.

iv) Les obligations en matière de sécurité s'appliquent au palier 2 (jusqu'au niveau Protégé B/intégrité moyenne, disponibilité moyenne ou préjudice moyen), sauf indication contraire.

c) Protection des données du Canada

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

d) Rôles et responsabilités liés à la sécurité

i) L'entrepreneur doit clairement délimiter les rôles et les responsabilités pour les contrôles de sécurité et les caractéristiques des services nuage entre l'entrepreneur et le Canada. Cela comprend, à tout le moins, les rôles et responsabilités pour : (i) la gestion des comptes, (ii) la protection des frontières, (iii) la sauvegarde des actifs et des systèmes d'information, (iv) la gestion des incidents, (v) la surveillance du système et (vi) la gestion des vulnérabilités.

ii) 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) lorsque les rôles et les responsabilités sont modifiés à la suite d'une modification des services nuage ou (iv) à la demande du Canada.

e) Assurance d'une tierce partie : Certifications et rapports

i) L'entrepreneur doit s'assurer que les données, l'infrastructure de l'entrepreneur (y compris les services IaaS, PaaS ou SaaS fournis au Canada) et les emplacements de service du Canada sont protégés au moyen de mesures de sécurité appropriées conformes aux exigences énoncées dans les pratiques et politiques de sécurité de l'entrepreneur.

ii) L'entrepreneur doit démontrer que les mesures sont conformes aux exigences énoncées dans les certifications et rapports de vérification suivants en fournissant des certifications ou des rapports d'évaluation par des tiers qui portent sur chaque couche de service (p. ex., IaaS, PaaS, SaaS) dans le cadre de l'offre de Services nuage, y compris :

(A) ISO/IEC 27001:2013 Technologies de l'information – Techniques de sécurité – Systèmes de gestion de la sécurité de l'information – Certification réalisée par un organisme de certification accrédité;

(B) ISO/IEC 27017:2015 Technologies de l'information – Techniques de sécurité – Code de bonnes pratiques pour les contrôles de sécurité de l'information fondés sur l'ISO/IEC 27002 pour les services du nuage – Certification réalisée par un organisme de certification accrédité;

(C) ISO/IEC 27018:2019 Techniques de sécurité – Code de bonnes pratiques pour la protection des informations personnelles identifiables (PII) dans l'informatique en nuage public agissant comme processeur d'IIPI;

(D) Rapport de vérification des contrôles d'une société de services (SOC) 2 de type II de l'AICPA (American Institute of Certified Public Accountants) pour les principes de confiance en matière de sécurité, de disponibilité, d'intégrité du traitement et de confidentialité – Produit par un comptable professionnel agréé indépendant.

iii) Chaque rapport de certification ou de vérification fourni doit : (i) indiquer le nom commercial légal de l'entrepreneur ou du sous-traitant concerné, (ii) indiquer la date de certification de l'entrepreneur ou du sous-traitant secondaire et le statut de cette certification; (iii) indiquer les services inclus dans la portée du rapport de certification. Si des exclusions sont déterminées ou s'il est nécessaire de séparer des organisations de sous-services, comme par exemple en ce qui concerne l'hébergement de centres de données, le rapport d'évaluation de l'organisation de sous-services doit être fourni.

iv) Chaque vérification donnera lieu à la production d'un rapport de vérification qui doit être mis à la disposition du Canada. Les certifications doivent être accompagnées de preuves à l'appui telles que le rapport d'évaluation ISO élaboré pour valider la conformité à la certification ISO et doivent clairement divulguer toutes les constatations de l'auditeur.

v) Chaque rapport de vérification SOC 2 de type II doit avoir été effectué dans les 12 mois précédant le début du contrat. Une lettre de transition peut être fournie pour démontrer que l'entrepreneur est en cours de renouvellement lorsqu'il y a un décalage entre la date du rapport de l'organisation de services et la fin de l'organisation utilisatrice (c'est-à-dire la fin de l'année civile ou de l'exercice financier).

vi) L'entrepreneur doit maintenir sa certification ISO 27001, ISO 27017, ISO/IEC 27018:2019 et SOC 2 de type II pendant toute la durée du contrat. L'entrepreneur doit fournir, au moins une fois par année, et sans délai à la demande du Canada, tous les rapports ou dossiers qui peuvent être raisonnablement requis pour démontrer que ses certifications sont à jour et valides.

f) Vérification de la conformité

i) L'entrepreneur doit effectuer des vérifications de confidentialité et de sécurité des ordinateurs, de l'environnement informatique et des centres de données physiques qu'il utilise pour traiter et protéger les données du Canada, comme suit :

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

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

(C) chaque vérification sera effectuée par des auditeurs indépendants qui (i) sont qualifiés en vertu du régime de certification AICPA, CPA Canada ou ISO et (ii) sont conformes à la norme ISO/IEC 17020 sur les systèmes de gestion de la qualité, au choix et aux frais de l'entrepreneur.

- ii) Chaque vérification donnera lieu à la production d'un rapport de vérification qui devra être mis à la disposition du Canada. Le rapport de vérification doit clairement divulguer toutes les constatations importantes de l'auditeur indépendant.
- iii) À la demande du Canada, des preuves supplémentaires telles que des plans de sécurité du système, des conceptions ou des documents d'architecture qui fournissent une description complète du système, peuvent être fournies par l'entrepreneur ou un sous-traitant secondaire afin de compléter les rapports de certification et de vérification décrits à la section 5 (Assurance d'une tierce partie) et ce, afin de démontrer la conformité de l'entrepreneur aux certifications requises par l'industrie.
- g) Programme d'évaluation de la sécurité des TI des fournisseurs de services d'infonuagique (FSI)
 - i) L'entrepreneur doit démontrer qu'il respecte les exigences de sécurité sélectionnées dans le profil de contrôle de la sécurité du GC pour les services informatiques du GC en nuage pour Protégé B, intégrité moyenne et disponibilité moyenne (PBMM) (<https://www.canada.ca/fr/gouvernement/systeme/gouvernement-numerique/innovations-gouvernementales-numeriques/services-informatique-nuage/profil-controle-securite-services-ti-fondes-information-nuage.html>) pour la portée des services via nuage 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 identifiées ci-dessous, et validées par des évaluations indépendantes par des tiers.
 - ii) La conformité sera évaluée et validée par Emploi et Développement social Canada (EDSC) (<https://cyber.gc.ca/fr/orientation/processus-devaluation-de-la-securite-des-technologies-de-linformation-sappliquant-aux>).
 - iii) L'entrepreneur doit démontrer qu'il a participé au processus en s'intégrant, en participant et en terminant avec succès au programme. Il lui faut fournir les documents suivants :
 - (A) une copie de la lettre de confirmation attestant qu'il participe au programme;
 - (B) une copie du plus récent rapport d'évaluation complété fourni par le gouvernement du Canada;
 - (C) la copie la plus récente du rapport sommaire fourni par le gouvernement du Canada.
 - iv) L'entrepreneur doit communiquer avec la Direction générale de l'innovation, de l'information et de la technologie d'EDSC, Sécurité de la technologie de l'information, pour toute information supplémentaire liée au programme d'évaluation de la sécurité des TI du Programme de sécurité des contrats (PSC).
 - v) En tout temps, l'entrepreneur a l'obligation d'informer EDSC lorsque des changements sont apportés aux offres de service via nuage.

vi) Si l'entrepreneur est un fournisseur de SaaS qui fait appel à un fournisseur de SaaS approuvé par le gouvernement du Canada (GC) qui se conforme déjà à la section 5 - Assurance par des tiers et à la section 7 (Programme d'évaluation de la sécurité informatique du fournisseur de services nuage, les sous-sections (1) et (2) le fournisseur de SaaS doit fournir au Canada une copie d'un courriel envoyé par le gouvernement du Canada confirmant que le soumissionnaire a terminé le Programme d'évaluation de la sécurité des TI des FSI.

h) Protection des données

i) L'entrepreneur doit :

(A) Mettre en œuvre le cryptage des données inactives pour les services via nuage hébergeant les données du Canada faisant en sorte que le cryptage des données inactives demeure en vigueur, sans interruption et actif en tout temps, même en cas de panne d'équipement ou technologique, conformément à la section 13 (Protection cryptographique).

(B) Transmettre les données du Canada de façon sécuritaire, incluant la capacité pour le GC de mettre en œuvre le cryptage des données en transit 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).

(C) Mettre en place des contrôles de sécurité qui limitent l'accès administratif aux données et aux systèmes du Canada par l'entrepreneur aux personnes qui ont un profil avec le besoin de savoir, y compris les personnes qui fournissent un soutien technique ou un service à la clientèle, et fournir au Canada un processus d'approbation pour accorder à un entrepreneur d'accéder aux données du Canada afin d'exécuter des activités de soutien, de maintenance ou d'exploitation.

(D) S'assurer que les ressources de l'entrepreneur ou des sous-traitants n'ont pas de droits d'accès permanents ou continus aux données du Canada et que l'accès soit limité aux ressources de l'entrepreneur ou des sous-traitants qui ont un besoin de savoir, y compris les ressources qui fournissent un soutien technique ou un service à la clientèle, en fonction de l'approbation du Canada.

ii) L'entrepreneur ne doit faire aucune copie des bases de données ou de toute partie de ces bases de données contenant des données du Canada en dehors des capacités de résilience du service régulier et dans les espaces ou zones régionales approuvés au Canada. En outre, l'entrepreneur doit s'assurer qu'aucun renseignement protégé B n'est traité à l'extérieur du Canada.

iii) L'entrepreneur doit s'assurer que tout traitement effectué à l'extérieur du Canada, y compris le déplacement ou la transmission de copies de données approuvées, sont effectués dans les régions de service convenues.

iv) 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.

i) Isolement des données

i) L'entrepreneur doit mettre en place des contrôles afin d'assurer l'isolement des ressources de sorte que les données du Canada ne se retrouvent pas mêlées aux données d'autres locataires, pendant l'utilisation, l'entreposage ou le transit, et dans tous les aspects des services nuage et de la fonctionnalité et du système de l'infrastructure de l'entrepreneur. et des services d'infonuagique, ainsi que de l'administration des systèmes. Cela comprend la mise en place de contrôles d'accès et l'application d'une séparation logique ou physique appropriée pour soutenir :

(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 à locataires multiples afin d'empêcher qu'un client malveillant ou compromis affecte le service ou les données des autres;

(C) la capacité du GC de soutenir l'isolement des locataires géré par le GC.

ii) À la demande du Canada, l'entrepreneur doit fournir un document qui décrit l'approche adoptée pour assurer l'isolement approprié des ressources, de sorte que les données du Canada ne soit pas mélangées aux données des autres locataires, pendant l'utilisation, l'entreposage ou le transit.

j) Emplacement des données

i) L'entrepreneur doit entreposer et protéger les données inactives du Canada, incluant les données sauvegardées ou conservées à des fins de redondance. Cela inclut la capacité d'isoler les données dans un centre de données approuvé situé au Canada. Un centre de données approuvé se définit comme suit :

(A) un centre de données qui répond à toutes les exigences et certifications de sécurité indiquées à la section 30 (Sécurité matérielle [centre de données et installations]);

(B) qui garantit l'impossibilité de trouver les données d'un client précis sur un support physique;

(C) qui utilise le cryptage afin d'assurer qu'aucune donnée n'est gravée sur disque qui n'est pas encrypté, conformément à la section 13 (Protection cryptographique).

- ii) L'entrepreneur doit attester que les services via nuage indiqués dans le contrat proviennent de pays membres de l'Organisation du Traité de l'Atlantique Nord (OTAN) (https://www.nato.int/cps/fr/nato/hq/nato_countries.htm) ou de l'Union européenne (UE) (https://europa.eu/european-union/about-eu/countries_fr) ou de pays avec lesquels le Canada a un instrument international bilatéral de sécurité industrielle. Le Programme de sécurité des contrats (PSC) a des instruments de sécurité industrielle bilatéraux internationaux avec les pays énumérés sur le site Web de SPAC suivant : <https://www.tpsgc-pwgsc.gc.ca/esc-src/international-fra.html> et qui est mis à jour périodiquement.
- iii) L'entrepreneur doit avoir la capacité d'isoler les données du Canada hébergées dans les services nuage dans des centres de données qui sont géographiquement situés au Canada.
- iv) À la demande du Canada, l'entrepreneur doit :
 - (A) fournir au GC une liste à jour des emplacements physiques, incluant la ville, qui peuvent entreposer les données inactives du Canada; et,
 - (B) identifier les parties des services nuage qui sont fournies depuis l'étranger, incluant tous les endroits où les données sont ~~entreposées~~ et traitées et d'où l'entrepreneur gère le service.
- v) L'entrepreneur des services nuage a l'obligation permanente d'aviser le Canada lors de mises à jour de la liste des emplacements physiques qui peuvent entreposer les données inactives du Canada.
- k) Transfert et récupération des données
 - i) L'entrepreneur doit fournir la capacité qui comprend les outils et services permettant au Canada de faire :
 - (A) extraire toutes les données du Canada en ligne, de proximité et hors ligne, comprenant mais sans s'y limiter, les bases de données, l'entreposage d'objets et de fichiers, les configurations de systèmes, les journaux d'activités nuage, le code source hébergé dans un dépôt de codes du Canada et les configurations du réseau de manière que les utilisateurs du Canada puisse utiliser les instructions afin de migrer d'un environnement à un autre.
 - (B) transférer sécuritairement toutes les données du Canada, comprenant les données de contenu et les métadonnées connexes, dans un format lisible et utilisable par machine, notamment le format CSV, et conformément aux lignes directrices de Bibliothèque et Archives Canada en formats de fichiers de transfert de ressources d'information de valeur durable (<https://www.bac-lac.gc.ca/fra/services/gestion-ressources-documentaires-documentation/lignes-directrices/Pages/lignes-directrices-formats-fichier-transferts-ressources-documentaires.aspx>).
- l) Élimination des données et retour des dossiers au Canada

i) L'entrepreneur doit, en toute sécurité, éliminer ou réutiliser les ressources (p. ex. équipement, entreposage de données, fichiers et mémoire) qui contiennent des données du Canada et s'assurer que les données entreposées antérieurement ne peuvent être traitées par d'autres clients après leur diffusion. Cela comprend toutes les copies de données du Canada qui sont faites à partir de reproductions aux fins de disponibilité élevée et de reprise après sinistre. L'élimination ou la réutilisation des ressources par l'entrepreneur doit correspondre à l'un des documents suivants :

ii) (i) National Industrial Security Program Operating Manual (DoD 5220.22-M6); (ii) Guidelines for Media Sanitization (NIST SP 800-88); (iii) Effacement et déclassification des supports d'information électroniques (ITSP.40.006 v2). À la demande du Canada, l'entrepreneur doit fournir un document décrivant son processus d'élimination ou de réutilisation des ressources.

iii) L'entrepreneur doit fournir au Canada une confirmation qui démontre qu'il a réussi à effacer, à purger ou à détruire toutes les ressources, selon le cas, et qu'il est en mesure d'empêcher le rétablissement de toute capacité (logiciel ou processus), de toute donnée, de toute information ou de tout système enlevé ou détruit une fois que le Canada aura cessé d'utiliser les services d'infonuagique.

m) Protection cryptographique

i) L'entrepreneur doit faire ce qui suit :

(A) Configurer toute cryptographie utilisée pour mettre en œuvre des garanties de confidentialité ou d'intégrité, ou utilisée dans le cadre d'un mécanisme d'authentification (par exemple, solutions RVP, TLS, modules logiciels, ICP et jetons d'authentification le cas échéant), conformément aux algorithmes de chiffrement approuvés par le Centre de sécurité des télécommunications (CST), ainsi qu'aux tailles des clés de chiffrement et aux cryptopériodes.

(B) Utiliser des algorithmes de chiffrement ainsi que des tailles de clé de chiffrement et des cryptopériodes qui ont été validés par le Programme de validation des algorithmes cryptographiques

(C) S'assurer que la cryptographie validée par la FIPS 140 est utilisée lorsque le chiffrement est nécessaire, et qu'elle est mise en œuvre, configurée et exploitée dans un module cryptographique, validé par le Programme de validation des modules cryptographiques (<https://cyber.gc.ca/fr/orientation/algothmes-cryptographiques-pour-linformation-non-classifie-protège-et-protège-b>) dans un mode soit approuvé soit autorisé pour fournir un degré élevé de certitude que le module cryptographique validé par la FIPS 140-2 fournit les services de sécurité attendus de la manière prévue.

(D) S'assurer que tous les modules utilisés validés par la FIPS 140-2 ont une certification active, actuelle et valide. Les produits conformes et validés par la norme FIPS 140 porteront des numéros de certificat.

n) Gestion des clés

L'entrepreneur doit veiller à ce qu'un service de gestion des clés puisse être mis à profit et offre notamment les capacités suivantes :

- i) une création/génération et une suppression des clés de chiffrement par le GC;
- ii) une définition et une application de politiques précises qui contrôlent la manière dont les clés peuvent être utilisées;
- iii) une protection de l'accès au matériel de chiffrement, y compris la prévention de l'accès de l'entrepreneur au matériel de chiffrement en clair;
- iv) la possibilité d'auditer tous les événements liés aux services de gestion des clés, y compris l'accès de l'entrepreneur aux fins d'examen par le Canada;
- v) la possibilité d'importer en toute sécurité des clés générées par le GC à partir d'un module de sécurité du matériel (HSM) géré par le GC sur place, sans exposer le texte en clair des clés pendant le processus d'importation;
- vi) la possibilité d'empêcher le fournisseur de services d'infonuagique de récupérer des copies en texte clair des clés générées par le GC;
- vii) la possibilité de déléguer les privilèges d'utilisation des clés aux services d'infonuagique utilisés pour les services gérés par le GC.

o) Protection des points terminaux

L'entrepreneur doit mettre en œuvre, gérer et surveiller les points terminaux à sécurité renforcée avec des protections actives fondées sur l'hôte pour prévenir les logiciels malveillants, les attaques et les abus, conformément aux directives de configuration reconnues par l'industrie, telles que celles qui se trouvent dans le NIST 800-123 (Guide to General Server Security), les normes du Center for Internet Security (CIS) ou une norme équivalente approuvée par écrit par le Canada.

p) 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 du cycle de vie des systèmes d'information et dans le développement de logiciels, de sites Web et de services, et qui est conforme aux normes et aux pratiques exemplaires de l'industrie, telles que (i) NIST, (ii) ISO 27034, (iii) ITSG-33, (iv) SAFECODE, ou (v) les normes de l'Open Web Application Security Project (OWASP) telles que l'Application Security Verification Standard (ASVS) ou une norme équivalente approuvée par écrit par le Canada. À la demande du Canada, l'entrepreneur doit fournir un document qui décrit le logiciel documenté de l'entrepreneur, ainsi que l'approche et le processus adoptés relativement au cycle de vie du développement du système.

q) Gestion de l'identité et des droits d'accès

- i) L'entrepreneur doit avoir la capacité pour le Canada de soutenir un accès sécurisé aux services d'infonuagique, y compris la capacité de configurer :
 - (A) l'authentification multi-facteurs conformément à la norme ITSP.30.031 V2 du CST (ou versions subséquentes) (<https://cyber.gc.ca/fr/orientation/guide-sur-l-authentification-des-utilisateurs-dans-les-systemes-de-technologie-de>) à l'aide de justificatifs approuvés par le GC;
 - (B) un accès en fonction du rôle;
 - (C) des contrôles d'accès aux objets entreposés;
 - (D) des politiques d'autorisation granulaire pour autoriser ou limiter l'accès.
 - ii) L'entrepreneur doit avoir la capacité d'établir des paramètres par défaut pour l'ensemble de l'organisation afin de gérer les politiques à l'échelle des locataires.
- r) Fédération
- i) L'entrepreneur doit permettre au Canada de soutenir l'intégration de l'identité fédérée. Pour ce faire, il doit notamment :
 - (A) prendre en charge les normes ouvertes relatives aux protocoles d'authentification tels que le Security Assertion Markup Language (SAML) 2.0 et l'OpenID Connect 1.0, ou ses versions ultérieures, où les justificatifs et authenticateurs des utilisateurs du GC pour les services d'infonuagique sont contrôlés uniquement par le Canada;
 - (B) permettre d'associer les identifiants uniques du Canada (p. ex. un numéro d'identification unique du Canada, une adresse de courriel du Canada) aux comptes d'utilisateurs des services d'infonuagique correspondants.
- s) Gestion des accès privilégiés
- i) L'entrepreneur doit :
 - (A) gérer et surveiller l'accès privilégié aux services d'infonuagique pour s'assurer que toutes les interfaces de service dans un environnement à locataires multiples sont protégées contre tout accès non autorisé, y compris celles qui sont utilisées pour héberger les services du GC;

- (B) restreindre et minimiser l'accès aux services d'infonuagique et aux données du Canada seulement aux appareils autorisés et aux utilisateurs finaux ayant explicitement besoin de cet accès;
- (C) appliquer et auditer les autorisations d'accès aux services d'infonuagique et aux données du Canada;
- (D) confiner 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;
- (E) mettre en œuvre des politiques sur les mots de passe afin de protéger les justificatifs d'identité contre les attaques en ligne ou hors ligne et de détecter ces attaques en consignait et en surveillant des événements tels que (i) l'utilisation réussie des justificatifs d'identité, (ii) l'utilisation inhabituelle de ces derniers et (iii) l'accès et l'exfiltration de la base de données des mots de passe, conformément à la version 3 (ou aux versions ultérieures) des Normes ITSP.30.031 du CST (<https://cyber.gc.ca/fr/orientation/guide-sur-lauthentification-des-utilisateurs-dans-les-systemes-de-technologie-de>);
- (F) mettre en œuvre des politiques sur les mots de passe afin de protéger les justificatifs d'identité contre les attaques en ligne ou hors ligne et de détecter ces attaques en consignait et en surveillant des événements tels que (i) l'utilisation réussie des justificatifs d'identité, (ii) l'utilisation inhabituelle de ces derniers et (iii) l'accès et l'exfiltration de la base de données des mots de passe, conformément à la version 3 (ou aux versions ultérieures) des Normes ITSP.30.031 du CST (<https://cyber.gc.ca/fr/orientation/guide-sur-lauthentification-des-utilisateurs-dans-les-systemes-de-technologie-de>);
- (G) mettre en place des mécanismes d'authentification multifacteur pour authentifier les utilisateurs ayant des privilèges d'accès, conformément à la version 3 (ou aux versions ultérieures) des Normes ITSP.30.031 du CST (<https://cyber.gc.ca/fr/orientation/guide-sur-lauthentification-des-utilisateurs-dans-les-systemes-de-technologie-de>);
- (H) mettre en place des mécanismes de contrôle de l'accès fondés sur les rôles pour attribuer des privilèges qui constituent la base de l'application de l'accès aux données du Canada;
- (I) définir et mettre en œuvre la séparation des tâches pour, au minimum, séparer les rôles de gestion des services et d'administration des rôles de soutien du système d'information, les rôles de développement des rôles opérationnels et les rôles de gestion de l'accès des autres rôles opérationnels;
- (J) adhérer aux principes du moindre privilège et du besoin de savoir pour accorder l'accès aux services d'infonuagique et aux données du Canada;
- (K) utiliser des points terminaux à sécurité élevée (ordinateurs, appareils d'utilisateurs finaux, serveurs intermédiaires, etc.) qui sont configurés de façon à offrir seulement des fonctions minimales (p. ex. un point terminal dédié qui ne peut pas

être utilisé pour naviguer sur Internet ou consulter ses courriels) afin de fournir le soutien et l'administration des services d'infonuagique et de l'infrastructure de l'entrepreneur;

- (L) mettre en place un processus automatisé pour effectuer un audit périodique de la création, de la modification, de l'activation, de la désactivation et de la suppression de comptes, au minimum;
- (M) révoquer, en cas de cessation d'emploi, les authentifiants et les justificatifs d'accès associés à tout personnel de services.

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

t) Gestion à distance

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

- (A) mettre en place des mécanismes d'authentification multi-facteurs pour authentifier les utilisateurs d'accès à distance, conformément à la version 3 (ou aux versions ultérieures) des Normes ITSP.30.031 du CST (<https://cyber.gc.ca/fr/orientation/guide-sur-lauthenticatation-des-utilisateurs-dans-les-systemes-de-technologie-de>);

- (B) employer des mécanismes cryptographiques pour protéger la confidentialité des séances d'accès à distance, conformément à la section 13 (Protection cryptographique);

- (C) acheminer tout l'accès à distance par des points de contrôle des accès gérés, surveillés et audités;

- (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.

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

u) Sécurité des réseaux et des communications

i) L'entrepreneur doit :

- (A) appliquer des connexions sécurisées aux services d'infonuagique, notamment en assurant la protection des données en transit entre le Canada et les services d'infonuagique au moyen de TLS 1.2 ou de versions ultérieures;
- (B) employer des protocoles ainsi que des algorithmes et des certificats cryptographiques pris en charge et à jour, comme le décrivent les normes ITSP.40.062 (<https://cyber.gc.ca/fr/orientation/conseils-sur-la-configuration-securisee-des-protocoles-reseau-itsp40062>) et ITSP.40.111
- (C) (<https://cyber.gc.ca/fr/orientation/algorithmes-cryptographiques-pour-linformation-non-classifie-protège-et-protège-b>);
- (D) utiliser des certificats correctement configurés dans les connexions TLS conformément aux directives du CST;
- (E) permettre au Canada de mettre en œuvre des contrôles d'accès au réseau et des règles de sécurité qui autorisent ou empêchent le trafic réseau vers les ressources canadiennes.

v) Journalisation et audit

- i) L'entrepreneur doit mettre en œuvre des pratiques et des contrôles de production et de gestion de journaux pour toutes les composantes des services d'infonuagique qui entreposent ou traitent les données du Canada, et qui sont conformes aux normes et aux pratiques exemplaires de l'industrie, comme celles de NIST 800-92 (Guide to Computer Security Log Management), le Guide sur la consignation d'événements (<https://www.canada.ca/fr/gouvernement/systeme/gouvernement-numerique/securite-confidentialite-ligne-sur-la-consignation-evenements.html>) ou une norme équivalente approuvée par écrit par le Canada. À la demande du Canada, l'entrepreneur doit fournir un document qui décrit ses pratiques et ses contrôles de production et de gestion de journaux documentés.
- ii) L'entrepreneur doit permettre au Canada d'exporter les journaux d'événements de sécurité au moyen d'interfaces d'établissement de rapports, de protocoles et de formats de données (Common Event Format [CEF], Syslog et autres formats communs) ainsi que d'interfaces de programmation d'application (API) normalisées qui permettent la récupération à distance des données de journaux (p. ex. par l'intermédiaire d'une interface de base de données qui utilise SQL) pour les services d'infonuagique utilisés, à l'appui des opérations du GC telles que la surveillance des services d'infonuagique et pour la preuve électronique et la mise en suspens pour raisons juridiques.
- iii) L'entrepreneur doit permettre au Canada d'examiner et d'analyser de manière centralisée les dossiers d'audit de multiples composants des services d'infonuagique utilisés par le client. Cela comprend le fait de fournir des interfaces API qui permettent d'inspecter et d'interroger les données inactives dans les applications SaaS, et notamment d'évaluer les

événements tels que l'accès et les comportements des utilisateurs et des administrateurs ainsi que les changements relatifs à l'accès des tiers aux interfaces API stockés dans les journaux des applications SaaS.

w) Surveillance continue

- i) L'entrepreneur doit continuellement gérer, surveiller et maintenir la posture de sécurité de l'infrastructure du fournisseur et des emplacements de service qui hébergent les données du Canada pendant toute la durée du contrat, et s'assurer que les services d'infonuagique fournis au Canada sont conformes aux présentes obligations en matière de sécurité. Dans le cadre de l'obligation, l'entrepreneur doit :
 - (A) surveiller activement et continuellement les menaces et les vulnérabilités pesant sur son infrastructure, les emplacements de service ou les données du Canada;
 - (B) déployer tous les efforts possibles pour prévenir les attaques au moyen de mesures de sécurité comme le refus de service;
 - (C) déployer tous les efforts possibles pour détecter les attaques, les incidents de sécurité et les autres événements anormaux;
 - (D) détecter l'utilisation et l'accès non autorisés à l'ensemble des services d'infonuagique, des données et des composants pertinents aux services d'infonuagique IaaS, PaaS ou SaaS du Canada;
 - (E) gérer et appliquer les correctifs et les mises à jour liés à la sécurité de manière opportune et systématique afin d'atténuer les vulnérabilités et de remédier à tout problème signalé publiquement dans les services d'infonuagique ou les bibliothèques que les services utilisent, et fournir des avis préalables liés aux correctifs conformément aux engagements convenus relatifs au niveau de service;
 - (F) réagir aux menaces et aux attaques contre ses services d'infonuagique, les contenir et veiller à la récupération;
 - (G) au besoin, prendre des contre-mesures proactives, y compris, des mesures préventives et d'intervention permettant d'atténuer les menaces.
 - ii) Les services d'infonuagique de l'entrepreneur doivent permettre de copier les données des applications du GC dans les services infonuagiques hébergés et de les acheminer vers un emplacement prédéterminé (dans le nuage ou dans les locaux du GC).
- x) Gestion des incidents de sécurité

- i) Le processus d'intervention en cas d'incident de sécurité de l'entrepreneur pour les services informatiques doit englober le cycle de vie de la gestion des incidents de sécurité en matière de TI et les pratiques de soutien pour les activités de préparation, de détection, d'analyse, de confinement et de reprise. Cela comprend ce qui suit :
- (A) Un processus d'intervention en cas d'incident de sécurité publié et documenté aux fins d'examen par le Canada, qui est conforme à l'une des normes suivantes : i) ISO/IEC 27035:2011 Technologies de l'information – Techniques de sécurité – Gestion des incidents de sécurité de l'information; ii) NIST SP800-612, Computer Security Incident Handling Guide (en anglais seulement); 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>); (iv) d'autres pratiques exemplaires issues des normes de l'industrie, si le Canada détermine, à sa discrétion, que celles-ci respectent ses exigences en matière de sécurité.
 - (B) Des processus et procédures documentés indiquant comment l'entrepreneur relèvera les incidents de sécurité, y donnera suite et y remédiera, dressera un rapport à leur sujet et les signalera au Canada, y compris : (i) la portée des incidents de sécurité de l'information que l'entrepreneur doit signaler au Canada; (ii) le degré de divulgation des incidents de sécurité de l'information détectés et les réponses connexes; (iii) le délai cible de signalement des incidents de sécurité de l'information; (iv) la procédure de signalement des incidents de sécurité de l'information; (v) les coordonnées des personnes-ressources pour le traitement des enjeux relatifs aux incidents de sécurité de l'information; (vi) tout recours applicable à certains incidents de sécurité de l'information.
 - (C) La capacité de l'entrepreneur d'appuyer les efforts d'enquête du Canada dans le cas de toute compromission des utilisateurs ou des données du service relevé.
 - (D) Cela permet uniquement aux représentants désignés du client autorisés (comme le Centre des opérations de sécurité de SPC) par le responsable technique :
 - (1) de demander et d'obtenir un accès et de l'information confidentiels en ce qui a trait aux données du client (données des utilisateurs, journaux d'événements du système et de sécurité, saisies de paquets du réseau ou de l'hôte, journaux de composants de sécurité comme des systèmes de détection et de prévention d'intrusion et des pare-feu, etc.), dans un format non chiffré, à des fins de réalisation d'enquêtes;
 - (2) d'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 d'informatique, y compris des procédures judiciaires et des mesures de protection pour la tenue d'une chaîne de possession.

- ii) À la demande du Canada, l'entrepreneur doit lui fournir un document qui décrit son processus d'intervention en cas d'incident de sécurité.
- iii) L'entrepreneur doit :
 - (A) collaborer avec les centres des opérations de sécurité du Canada (p. ex. Centre canadien pour la cybersécurité et centre des opérations de sécurité ministériel) en ce qui concerne le confinement, l'élimination et la reprise en cas d'incident de sécurité, conformément au processus d'intervention en cas d'incident de sécurité;
 - (B) tenir un registre des violations de la sécurité comprenant une description des violations et indiquant leur durée, leurs conséquences, le nom de la personne ayant signalé la violation, la personne à qui elle a été signalée, et la procédure suivie pour récupérer les données ou rétablir le service;
 - (C) assurer le suivi des divulgations de données canadiennes ou permettre au Canada d'en assurer le suivi, y compris les données qui ont été divulguées, à qui elles l'ont été, et à quel moment.
- iv) Le Canada pourrait exiger des preuves judiciaires de la part de l'entrepreneur pour contribuer à une enquête du GC. L'entrepreneur convient de fournir de l'aide au GC dans la mesure du possible.
- y) Intervention en cas d'incident de sécurité
 - i) L'entrepreneur doit alerter et aviser promptement le Canada (par téléphone ou par courriel) de toute compromission, de toute violation ou de toute preuve comme (i) un incident de sécurité, (ii) une défectuosité liée à la sécurité d'un actif, (iii) l'accès irrégulier ou non autorisé à un actif, (iv) la copie à grande échelle d'un actif d'information ou (v) toute autre activité illégale recensée par l'entrepreneur, portant ce dernier à croire de manière raisonnable que le risque de compromission ou 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.
 - ii) Si l'entrepreneur prend connaissance de toute compromission ou de toute violation et qu'il relève une violation de la sécurité entraînant la destruction, la perte, l'altération ou la divulgation non autorisée des données du client ou de données personnelles ou l'accès accidentel ou illégal à ces données pendant son traitement de celles-ci (chacun étant un « incident de sécurité »), il doit rapidement et sans tarder (i) informer le Canada de cet incident de sécurité, (ii) mener une enquête et fournir des renseignements détaillés au Canada sur cet incident de sécurité, et (iii) prendre les mesures raisonnables pour remédier aux causes et atténuer les dommages découlant de l'incident de sécurité.
- z) Fuite d'information

- i) L'entrepreneur doit avoir un processus documenté qui énonce son approche en cas d'incident de fuite d'information. Le processus doit être harmonisé i) au document ITSG-33, Contrôles de sécurité relativement à la section IR-9, Intervention en cas de fuite d'information et Étapes pour gérer les fuites de données dans le nuage (ITSAP.50.112) <https://www.cyber.gc.ca/fr/orientation/etapes-pour-gerer-les-fuites-de-donnees-dans-le-nuage-itsap50112>, ou ii) à une autre norme de l'industrie approuvée par écrit par le Canada. Nonobstant ce qui précède, le processus d'intervention en cas de fuite d'information de l'entrepreneur doit comprendre, à tout le moins :
- (A) un processus d'identification des éléments de données précis utilisés dans la contamination d'un système;
 - (B) un processus visant à isoler et à éradiquer un système contaminé;
 - (C) un processus d'identification des systèmes pouvant avoir été subséquemment contaminés et toute autre mesure prise pour empêcher la propagation de la contamination.
- ii) À la demande du Canada, l'entrepreneur doit lui fournir un document qui décrit son processus d'intervention en cas de fuite d'information.
- aa) Tests de sécurité et validation
- i) L'entrepreneur doit disposer d'un processus qui permet au Canada d'effectuer une analyse de vulnérabilité ou un essai de pénétration non perturbateur et non destructif visant la partie canadienne des composantes des services d'infonuagique dans l'environnement de l'entrepreneur.
- ii) L'entrepreneur doit offrir la possibilité de mettre en place un outil libre-service de vérification de l'état de la sécurité ou un outil de notation qui permet de mesurer la posture de sécurité des services d'infonuagique configurés par le Canada.
- bb) Filtrage de sécurité du personnel
- i) L'entrepreneur doit veiller à la mise en place de mesures de sécurité qui accordent et maintiennent le niveau de filtrage de sécurité requis pour son personnel participant à la prestation des services d'infonuagique et pour le personnel du sous-traitant, en fonction de leurs privilèges d'accès aux actifs des systèmes d'information sur lesquels les données du Canada sont entreposées et traitées.
- ii) Les mesures de contrôle de l'entrepreneur doivent être appliquées conformément à la définition et aux pratiques énoncées dans la Norme sur le filtrage de sécurité du Conseil du Trésor (<https://www.tbs-sct.gc.ca/pol/doc-fra.aspx?id=28115>), ou utiliser un équivalent acceptable convenu par le Canada.

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

- (A) une description des postes des employés et des sous-traitants qui ont besoin d'un accès aux données du client ou qui ont la capacité d'influencer la confidentialité, l'intégrité ou la disponibilité des services d'infonuagique;
- (B) une description des activités et des pratiques de filtrage de sécurité, y compris les procédures de notification qui doivent être suivies si le filtrage n'a pas été achevé ou si les résultats entraînent des doutes ou des préoccupations;
- (C) une description de la sensibilisation et de la formation en matière de sécurité dans le cadre de l'intégration à l'emploi, lorsque les rôles des employés et des sous-traitants changent, et de façon continue, pour s'assurer que les employés et les sous-traitants 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 initiés malveillants potentiels et les contrôles mis en œuvre pour atténuer le risque d'accès aux données du GC ou de dommage à la fiabilité des services d'infonuagique hébergeant les données du Canada.

cc) Sécurité matérielle (centre des données et installations)

- i) L'entrepreneur doit veiller à la mise en place de mesures de sécurité matérielle qui assurent la protection des installations de TI et des actifs du système d'information dans lesquels les données du Canada sont entreposées et protégées contre toute forme de manipulation, de perte, de dommages et de saisie. Des mesures de protection matérielle visant toutes les installations qui hébergent des données du Canada doivent être appliquées conformément à une approche fondée sur les risques reposant sur la prévention, la détection, l'intervention et la récupération en matière de sécurité matérielle ou utiliser une telle approche, conformément aux mesures de contrôle et aux pratiques en matière de sécurité matérielle figurant à l'appendice C de la [Directive](https://www.tbs-sct.gc.ca/pol/doc-fra.aspx?id=32611) (<https://www.tbs-sct.gc.ca/pol/doc-fra.aspx?id=32611>). Les mesures de sécurité exigées en vertu de cette disposition comprennent, à tout le moins :
 - (A) des capacités suffisantes de redondance et de reprise dans les installations de l'entrepreneur et entre celles-ci, qui sont suffisamment disparates sur le plan géographique pour que la perte d'une installation n'empêche pas la récupération des données et des données du Canada conformément aux engagements sur les niveaux de service convenus;

- (B) l'utilisation adéquate des supports de TI, conformément à l'annexe B du [Guide sur la catégorisation de la sécurité des services fondés sur l'infonuagique \(ITSP.50.103\)](#) – [Centre canadien pour la cybersécurité](#);
 - (C) le contrôle de la maintenance de tous les systèmes d'information et de leurs composants pour protéger leur intégrité et assurer leur disponibilité continue;
 - (D) le contrôle de l'accès aux dispositifs de sortie des systèmes d'information pour empêcher l'accès non autorisé aux données du Canada;
 - (E) la restriction de l'accès physique aux données du Canada et aux emplacements de services d'infonuagique au personnel de service autorisé en fonction du poste ou du rôle et du principe du besoin d'accès et validé par deux formes d'identification;
 - (F) l'escorte des visiteurs et la surveillance de leurs activités;
 - (G) l'application de mesures de protection des données du GC à d'autres lieux de travail (p. ex. les sites de télétravail);
 - (H) la ~~conservation~~ l'enregistrement et la surveillance de tous les accès physiques aux points de service et de tous les accès logiques aux systèmes qui hébergent les données du Canada, au moyen d'une combinaison de registres d'accès et de mécanismes de vidéosurveillance dans toutes les zones sensibles et de détection des intrusions.
- ii) À la demande du Canada, l'entrepreneur doit lui fournir un document qui décrit ses mesures de sécurité matérielle.
 - iii) L'entrepreneur doit aviser le Canada de tout changement apporté aux mesures de sécurité matérielle qui pourrait nuire de manière importante à la sécurité matérielle. Le Canada se réserve le droit de résilier le contrat pour manquement s'il détermine que l'entrepreneur ne satisfait pas aux exigences en matière de sécurité matérielle précisées dans le contrat.
- dd) Gestion des risques de la chaîne d'approvisionnement
- i) L'entrepreneur doit veiller à ce que des mesures de sécurité soient prises pour atténuer les menaces et les vulnérabilités associées à la chaîne d'approvisionnement des services de TI en vue de préserver la confiance en ce qui concerne la sécurité des sources des systèmes d'information et les composants de TI servant à offrir les services d'infonuagique. En font notamment partie la conception et la mise en œuvre de contrôles visant à atténuer et à contenir les risques liés à la sécurité des données par une séparation adéquate des tâches, un accès établi selon les fonctions des utilisateurs et un accès qui suit le principe du privilège minimal pour tout le personnel au sein de la chaîne d'approvisionnement.
 - ii) L'entrepreneur doit avoir une approche de gestion des risques de la chaîne d'approvisionnement (GRCA), dont un plan de GRCA qui est conforme à l'une des pratiques exemplaires suivantes :

- (A) ISO/IEC 27036 Technologies de l'information – Techniques de sécurité – Sécurité d'information pour la relation avec le fournisseur (parties 1 à 4);
 - (B) Publication spéciale 800-161 du NIST – Supply Chain Risk Management Practices for Federal Information Systems and Organizations;
 - (C) Contrôle de sécurité ITSG-33 pour SA-12 lorsque les garanties de sécurité définies sont documentées dans un plan de GRCA.
- iii) Dans les 90 jours suivant l'attribution du contrat, l'entrepreneur doit :
- (A) présenter une preuve confirmant que l'approche et le plan de GRCA ont été évalués et validés par un tiers indépendant certifié selon les exigences de l'AICPA, de CPA Canada ou du régime de certification ISO
- OU
- (B) présenter au Canada une copie du plan de GRCA, annuellement ou sur demande du Canada.
- iv) Dans les cas où l'entrepreneur est un fournisseur de SaaS utilisant un fournisseur d'laaS approuvé par le GC qui se conforme déjà aux exigences de la section 31 (Gestion des risques de la chaîne d'approvisionnement), le fournisseur de SaaS utilisant un fournisseur d'laaS approuvé par le GC doit fournir dans les 90 jours suivant l'attribution du contrat une liste de produits de technologie de communication de l'information (TCI) qui décrit l'équipement de TCI déployé dans l'environnement laaS approuvé par le GC pour un examen de l'intégrité de la chaîne d'approvisionnement (ICA). Cet examen de l'ICA sera effectué au plus tôt tous les trois ans.
- ee) Fuite d'information
- i) Le processus de l'entrepreneur relatif aux incidents de fuite d'information doit être harmonisé aux directives de la section IR-9, Intervention en cas de fuite d'information, du document ITSG-33, Contrôles de sécurité. Le processus de l'entrepreneur relatif aux incidents de fuite d'information doit comprendre, à tout le moins :
 - (A) un processus d'identification des éléments de données précis utilisés dans la contamination d'un système;
 - (B) un processus visant à isoler et à éradiquer un système contaminé;

- (C) un processus permettant de déterminer les systèmes et l'actif d'information particulier pouvant avoir été subséquemment contaminés et toute autre mesure prise pour empêcher la propagation de la contamination.
- (D) L'entrepreneur confirmera un point de contact, les procédures appropriées et une forme de communication sécurisée convenue pour fournir de l'aide aux administrateurs du client lorsque cela est possible.
- ii) L'entrepreneur doit fournir au Canada un processus relatif aux incidents de fuite d'information à jour tous les ans ou rapidement après toute modification apportée à son processus relatif aux incidents de fuite d'information.
- ff) Séparation des données
 - i) L'entrepreneur doit mettre en place des contrôles pour assurer l'isolation appropriée des ressources, de sorte que les actifs d'information ne soient pas mélangés avec les données d'autres locataires, qu'ils soient en cours d'utilisation, de stockage ou de transit, ainsi que dans tous les aspects des fonctionnalités des services et de l'infrastructure du fournisseur et de l'administration des systèmes. Cela inclut la mise en œuvre de contrôles d'accès et l'application de la séparation logique ou physique appropriée pour prendre en charge :
 - (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 des environnements à locataires multiples afin d'empêcher que les activités d'un client malveillant ou compromis aient de répercussions sur le service ou les données d'un autre.
- gg) Protection des données
 - L'entrepreneur doit aviser le Canada lorsqu'il y a des mises à jour de la liste des emplacements physiques qui peuvent contenir des données du Canada.

PARTIE 7 – CLAUSES DU CONTRAT SUBSÉQUENT

7.1 Besoin

L'entrepreneur consent à offrir les services et à effectuer les travaux décrits dans le contrat ainsi que dans l'énoncé des travaux, conformément au contrat et aux prix énoncés dans ce dernier.

7.2 Services

L'entrepreneur s'engage à offrir le service décrit à l'annexe A – Énoncé des besoins, ce qui comprend au moins :

- (1) l'accès de l'utilisateur à la solution de logiciel-service décrite dans le contrat;
- (2) la documentation de la solution;
- (3) la maintenance, la mise à niveau et la mise à jour de la solution;
- (4) la gestion des incidents et des défauts garantissant le fonctionnement de la solution aux niveaux de service applicables;
- (5) les services requis d'infrastructure de technologie de l'information accessoires et supplémentaires;
- (6) les services d'infrastructure nécessaires pour livrer la solution; et
- (7) des services professionnels et de la formation, à la demande du Canada.

7.3 Services professionnels

L'entrepreneur s'engage à fournir les services professionnels (le 'travail') suivants, sur demande du Canada, à l'aide du processus d'autorisation de tâches :

- (1) les services de mise en œuvre, dont la configuration, la migration, l'aide au déploiement, l'aide aux tests d'approbation et la transition à l'état de fonctionnement réel, comme définis dans l'énoncé des besoins;
- (2) les services de formation.

7.4 Intégralité de l'entente

Le contrat constitue l'entente complète et unique intervenue entre les parties et remplace toutes les négociations, communications ou autres ententes, écrites ou verbales, à moins qu'elles ne soient incorporées par renvoi au contrat. Seuls les engagements, représentations, déclarations et conditions qui figurent au contrat lient les parties.

7.5 Client

Le client initial est Emploi et Développement social Canada (EDSC). Toutefois, l'autorité contractante peut progressivement ajouter des clients, y compris tout ministère ou toute société d'État mentionnés dans la *Loi sur la gestion des finances publiques* (et ses modifications), et toute autre partie au nom de laquelle le ministère des Travaux publics et des Services gouvernementaux est autorisé à agir en vertu de l'article 16 de la Loi sur le ministère des Travaux publics et des Services gouvernementaux.

7.6 Réorganisation des clients

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

7.7 Durée déterminée et renouvellement automatique

- (1) **Période du contrat.** La durée du contrat comprend la période pendant laquelle l'entrepreneur est tenu d'offrir les services et d'effectuer les travaux.
- (2) **Durée initiale.** Le contrat débute à la date d'attribution du contrat et se termine trois (3) an plus tard.
- (3) **Périodes d'option.** L'entrepreneur accorde au Canada l'option irrévocable de prolonger la durée du contrat pour au plus sept (7) période(s) supplémentaire(s) d'un (1) an selon les mêmes conditions. L'entrepreneur accepte que pendant la période prolongée du contrat, il soit payé conformément aux dispositions applicables énoncées dans la base de paiement. Le Canada peut exercer cette option à n'importe quel moment, en envoyant un avis écrit à l'entrepreneur au moins deux (2) jours civils avant la date d'expiration du contrat. L'option ne pourra être exercée que par l'autorité contractante et sera confirmée, pour des raisons administratives seulement, par une modification au contrat.
- (4) **Option de non-participation au renouvellement automatique.** Par les présentes, le Canada avise l'entrepreneur qu'il renonce à tout renouvellement automatique de l'obligation à terme. L'entrepreneur accuse réception de l'avis et déclare que le présent contrat ne sera valide que jusqu'à l'expiration du contrat, comme indiqué précédemment.

7.8 Rigueur dans les délais

- (1) Il est essentiel que les services soient rendus dans les délais prévus au contrat.
- (2) Il est essentiel que les travaux soient menés conformément aux délais prévus dans une autorisation de tâche.

7.9 Résiliation pour des raisons de commodité

- (1) L'autorité contractante peut, à tout moment avant la fin des services, en donnant un avis écrit à l'entrepreneur, résilier le contrat ou une partie du contrat pour des raisons de commodité. Une fois un tel avis de résiliation donné, l'entrepreneur doit se conformer aux exigences prévues dans l'avis de résiliation. Si le contrat est résilié en partie seulement, l'entrepreneur doit poursuivre l'exécution des services qui ne sont pas touchés par l'avis de résiliation. La résiliation prendra effet immédiatement ou, le cas échéant, au moment prévu dans l'avis de résiliation.
- (2) Si un avis de résiliation est donné en vertu du paragraphe 1, l'entrepreneur aura le droit de se faire payer les coûts raisonnablement et dûment engagés pour l'exécution du contrat dans la mesure où il n'a pas déjà été payé ou remboursé par le Canada. L'entrepreneur s'engage à ne recevoir que les montants suivants :
 - (a) sur la base du prix contractuel, pour toute partie des travaux effectués qui ont été inspectés et acceptés conformément au contrat, qu'ils aient été complétés avant l'avis de résiliation ou après celui-ci conformément aux directives contenues dans l'avis de résiliation;
 - (b) les coûts engagés par l'entrepreneur, plus un profit juste et raisonnable tel que déterminé à l'article 10.65 du Guide des approvisionnements de TPSGC (calcul du profit des contrats négociés, pour toute partie des travaux entrepris, mais non terminés, avant la date du préavis). L'entrepreneur convient qu'il n'a droit à aucun profit prévu sur toute partie du marché résiliée;
 - (c) les frais liés à la résiliation des travaux engagés par l'entrepreneur, en excluant les coûts des indemnités de cessation d'emploi ou des dommages pour les employés dont les services ne sont plus requis, à l'exception des salaires que l'entrepreneur est obligé de verser en vertu de la loi.
- (3) Le Canada peut réduire le montant du paiement effectué à l'égard de toute partie des travaux, si après inspection, elle ne satisfait pas aux exigences du contrat.

- (4) Les sommes auxquelles l'entrepreneur a droit selon le présent article et les sommes versées ou dues à l'entrepreneur ne doivent pas dépasser, au total, le prix contractuel. Sauf dans la mesure prévue dans le présent article, l'entrepreneur n'aura aucun recours et ne pourra donc toucher aucune compensation ou indemnité ni obtenir de dommages-intérêts en cas de perte de profit découlant de tout avis de résiliation en vertu du présent article. L'entrepreneur s'engage à rembourser immédiatement au Canada la portion de tout paiement anticipé non liquidée à la date de la résiliation.
- (5) L'entrepreneur doit s'assurer que les données EMAS seront disponibles au Canada, au format CSV pouvant être rapatrié au Canada, pendant trois (3) mois après l'annulation de l'accès.

7.10 Accès à l'information

Les documents créés par l'entrepreneur et dont le Canada assume le contrôle sont assujettis aux dispositions de la *Loi sur l'accès à l'information*. L'entrepreneur reconnaît les responsabilités du Canada en vertu de la *Loi sur l'accès à l'information* et doit, dans la mesure du possible, aider le Canada à s'acquitter de ces responsabilités. De plus, l'entrepreneur reconnaît que l'article 67.1 de la *Loi sur l'accès à l'information* stipule que toute personne qui détruit, modifie, falsifie ou cache un document ou ordonne à une autre personne de commettre un tel acte, dans l'intention d'entraver le droit d'accès prévu à la *Loi sur l'accès à l'information*, est coupable d'un acte criminel passible d'un emprisonnement ou d'une amende, ou les deux.

<https://laws-lois.justice.gc.ca/fra/lois/A-1/>

7.11 Solution

- (1) **Logiciel-service.** L'entrepreneur livrera la solution à l'aide d'un modèle de livraison de logiciel-service permettant au Canada d'accéder à la solution hébergée par l'entrepreneur et de l'utiliser.
- (2) **Solution commercialement disponible.** Le Canada reconnaît que la solution est une solution commercialement disponible offerte à d'autres clients. Dans le cadre de son abonnement pour utiliser la solution, l'entrepreneur s'engage à mettre à la disposition du Canada toutes les fonctions et fonctionnalités que comprend la version disponible dans le commerce, ainsi que les services d'infrastructure informatique auxiliaires et nécessaires à la prestation de la solution, le tout étant compris dans le prix de l'abonnement.
- (3) **Évolution de l'application logicielle; caractéristiques ou fonctionnalités.** Le Canada reconnaît que la solution, l'application logicielle sous-jacente ou l'infrastructure associée peut évoluer pendant la durée du contrat. L'entrepreneur convient de continuer à fournir le service sous forme de solution commercialement disponible, avec des fonctionnalités ou des caractéristiques et à des conditions qui ne sont pas moins favorables qu'au moment de l'attribution du contrat.
- (4) **Améliorations et évolution de la solution.** Les parties reconnaissent que la technologie et les modèles d'affaires évoluent rapidement et que toute solution fournie au début de la durée du contrat sera inévitablement différente de la solution fournie à la fin de la durée du contrat, et que la ou les méthodes par lesquelles la solution et tout périphérique potentiel sont livrés au Canada soient susceptibles de changer ou d'évoluer et que, au moment de la conclusion du présent contrat, les parties ne puissent envisager tous les biens ou services qui peuvent être livrés aux termes du présent contrat, mis à part le fait qu'ils seront livrés aux utilisateurs. Dans cet esprit, les parties s'entendent sur ce qui suit :
- (a) L'entrepreneur doit maintenir et améliorer continuellement la solution et l'infrastructure tout au long de la durée du contrat sur une base commercialement raisonnable, et doit fournir ces améliorations et améliorations au Canada dans le cadre de l'abonnement du Canada, sans ajustement de prix si ces améliorations et améliorations sont également offertes aux autres clients sans frais supplémentaires.

- (b) Si l'entrepreneur supprime des fonctions de l'offre commerciale de la solution et les offres dans tout autre service ou produit, ou tout service ou produit nouveau, il doit continuer de les fournir au Canada dans le cadre de l'abonnement du Canada aux services, selon les modalités actuelles du contrat, peu importe si ces autres services ou produits contiennent également des fonctions nouvelles ou additionnelles. L'entrepreneur n'est pas tenu de se conformer au présent paragraphe si la solution acquise par le Canada est toujours offerte par l'entrepreneur parallèlement aux nouveaux services offerts aux autres clients.
- (5) L'entrepreneur doit voir à ce que les mises à niveau et les mises à jour du SAGU :
- (a) n'entraînent pas de travaux supplémentaires pour le Canada, à l'exception des essais applicables;
 - (b) n'entraînent pas de pertes de données, de documents électroniques ou de comptes d'utilisateur du Canada.

7.12 Services

7.12.1 Services de la solution

- (1) **Logiciel-service.** L'entrepreneur fournira tous les services dont le Canada a besoin pour accéder à la solution et l'utiliser, selon ce qui est précisé dans le contrat.
- (2) **Autorité.** L'entrepreneur déclare et garantit qu'il possède ou qu'il a obtenu et conservera pendant toute la durée du contrat tous les pouvoirs nécessaires, notamment les droits de propriété intellectuelle requis pour fournir les services conformément aux modalités du présent contrat.
- (3) **Indemnisation.** L'entrepreneur convient d'indemniser le Canada de toutes les pertes et dépenses (y compris les frais juridiques) découlant de toute réclamation pour violation de propriété intellectuelle par un tiers fondée sur l'utilisation de la solution par le Canada.
- (4) **Accessibilité :** L'entrepreneur doit s'assurer que la solution n'entrave pas au respect des normes, tel qu'il est précisé dans la Norme sur l'accessibilité des sites Web : <https://www.tbs-sct.gc.ca/pol/doc-fra.aspx?id=23601>.
- (5) **Octroi des droits d'utilisation.** L'entrepreneur accorde au Canada le droit non exclusif et incessible d'accéder à la solution et de l'utiliser à partir d'un nombre illimité d'emplacements, d'appareils et d'environnements d'exploitation, au moyen d'une connexion sécurisée, sans fil, mobile ou autre, au moyen d'un navigateur Web ou d'une autre technologie de connexion qui pourrait devenir disponible.
- (6) **Inclusions.** L'entrepreneur déclare et certifie que les services comprennent ce qui suit :
- (a) L'hébergement et la tenue à jour de la solution;
 - (b) La prestation de tous les services d'infrastructure de la technologie de l'information accessoires et supplémentaires requis, conformément à toutes les normes de sécurité requises;
 - (c) L'infrastructure technique qui respecte toutes les normes de sécurité requises, permettant au Canada d'utiliser la solution pour traiter les données de clients conformément à ses normes de sécurité exprimées;
 - (d) Un accès et une utilisation absolues par le client, indépendamment de la quantité de données créées, traitées ou stockées par la solution;
 - (e) Tous ces éléments étant inclus dans le prix.

- (7) **Droits d'utilisation restreints.** Le Canada reconnaît qu'en fournissant les services, l'entrepreneur ne délivre aucun droit de propriété sur un produit logiciel, une composante de la solution ou une infrastructure utilisés par l'entrepreneur pour fournir les services, sauf dans les cas expressément prévus dans une autorisation de tâches. Le Canada ne fera pas sciemment ce qui suit :

- (a) Distribuer, octroyer une licence, prêter ou vendre la solution;
- (b) Porter atteinte aux mécanismes de sécurité de la solution ou les contourner; ou

- (c) Retirer, modifier ou obscurcir tout avis de droit d'auteur, de marque commerciale ou tout autre avis de propriété figurant sur ou dans la solution.

(8) **Modalités applicables.** L'entrepreneur a indiqué, et le Canada a reconnu que l'entrepreneur peut modifier unilatéralement les modalités selon lesquelles il fournit son offre commerciale de la solution, sans préavis à ses clients, dont le Canada. L'entrepreneur déclare et garantit qu'une telle modification n'entraînera pas des conditions moins favorables, notamment en ce qui concerne le prix, les niveaux de service et les recours, sans égard à tout avis contraire.

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

(10) **Offre de logiciel-service commercial.** Le Canada reconnaît qu'il acceptera l'offre de logiciel-service commercial d'entrepreneur et déclare que, à moins que cela soit explicitement désigné comme travaux ou services à fournir en vertu du présent contrat, le Canada n'exige pas de développement personnalisé, de services de rechange, de niveaux de service, de fonctionnalités ou de caractéristiques.

7.12.2 Niveau de services

(1) **Annexe I.** L'accord sur les niveaux de service (présenté par l'entrepreneur), contient les renseignements précis qui définissent les niveaux et les normes relatifs aux processus et aux attentes en matière de rendement pour les services devant être fournis en vertu du contrat, et doit être lu conjointement avec la section suivante :

- (a) **Crédits de service.** L'entrepreneur accordera au Canada les crédits de service applicables s'il n'atteint pas les niveaux de disponibilité de la solution de temps de disponibilité définis à l'annexe F, Accord sur les niveaux de service.
- (b) **Exclusions.** L'entrepreneur précisera expressément toute exclusion des niveaux de disponibilité de la solution indiqués à l'annexe F, Accord sur les niveaux de service.
- (c) **Services de soutien.** L'entrepreneur fournira un soutien technique, **en français et en anglais**, en stricte conformité avec l'annexe F, Accord sur les niveaux de service.
- (d) **Acheminement.** L'entrepreneur peut prévoir un processus de recours hiérarchique pour le règlement des différends, qui est décrit à l'annexe F, Accord sur les niveaux de service.
- (e) **Pas d'infraction.** L'entrepreneur garantit que rien dans la solution, ou dans l'utilisation de la solution par le Canada, ne constitue ou ne constituera une appropriation illicite de la propriété intellectuelle ou des autres droits d'un tiers ni ne les enfreindra.

7.12.3 Documents

- (1) **Documentation sur la solution.** L'entrepreneur doit fournir au Canada, au moment de l'attribution du contrat, l'accès à la documentation, en anglais, sur la solution commercialement disponible. L'entrepreneur doit mettre à jour la documentation sur la solution à des conditions raisonnables sur le plan commercial.
- (2) **Autres documents.** L'entrepreneur doit fournir toute documentation nécessaire à l'exécution des travaux, ou y donner accès.

7.12.4 Droits de traduction

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

7.12.5 Droits moraux

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

7.12.6 Documentation défectueuse

Si, à tout moment pendant le contrat, le Canada avise l'entrepreneur d'un défaut ou d'une non-conformité dans une partie de la documentation livrée avec les travaux, l'entrepreneur corrigera le défaut ou la non-conformité dès que possible, et à ses propres frais. Le Canada peut fournir à l'entrepreneur des renseignements sur des défauts ou des aspects non conformes dans d'autres documents, y compris la documentation de la solution, à titre d'information seulement.

7.12.7 Exécution des travaux

Garantie. L'entrepreneur déclare et atteste ce qui suit : a) il a les compétences pour exécuter les travaux; b) il dispose de tout ce qui est nécessaire pour exécuter les travaux, y compris les ressources, les installations, la main-d'œuvre, la technologie, l'équipement et les matériaux; c) il a les qualifications nécessaires, y compris les connaissances, les compétences, le savoir-faire et l'expérience, pour exécuter les travaux avec efficacité.

7.12.8 Recours

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

7.12.9 Sous-traitants

(1) **Conditions de sous-traitance.** L'entrepreneur peut sous-traiter l'exécution des travaux, mais seulement si a) l'entrepreneur obtient le consentement écrit préalable de l'autorité contractante, b) le sous-traitant est lié par les modalités du présent contrat, et c) l'entrepreneur demeure responsable envers le Canada pour tous les travaux effectués par le sous-traitant.

(2) **Exceptions au consentement de sous-traitance.** L'entrepreneur n'est pas tenu d'obtenir le consentement de l'autorité contractante à l'égard des contrats de sous-traitance expressément autorisés dans le contrat. L'entrepreneur peut également, sans le consentement de l'autorité contractante : i) acheter des produits courants en vente libre dans le commerce, ainsi que des articles et des matériaux produits par des fabricants dans le cours normal de leurs affaires; ii) sous-traiter tous les services accessoires qui seraient normalement sous-traités dans l'exécution des travaux; et iii) permettre à ses sous-traitants à tout échelon d'effectuer des achats ou de sous-traiter comme le prévoient les alinéas i) et ii).

7.12.10 Retard justifiable

(1) **Absence de responsabilité.** L'entrepreneur n'est pas responsable des retards d'exécution ni de l'inexécution due à des causes indépendantes de sa volonté qui ne pouvaient raisonnablement être prévues ou évitées par des moyens raisonnablement accessibles à l'entrepreneur, pourvu que l'entrepreneur avise l'autorité contractante du retard ou de la probabilité du retard dès qu'il en prend connaissance (ce qu'on appelle « retard justifiable »).

(2) **Avis.** L'entrepreneur doit de plus informer l'autorité contractante, dans les 15 jours ouvrables, de toutes les circonstances liées au retard et soumettre à l'approbation de l'autorité contractante un plan de redressement clair qui détaille les étapes que l'entrepreneur propose de suivre afin de réduire au minimum les conséquences de l'événement qui a causé le retard.

(3) **Dates de livraison et échéances.** Toute date de livraison ou autre date qui est directement touchée par un retard justifiable fera l'objet d'un report raisonnable dont la durée n'excédera pas la durée du retard justifiable.

(4) **Le Canada est non-responsable des frais.** Le Canada ne sera pas responsable des frais engagés par l'entrepreneur ou l'un de ses sous-traitants ou mandataires par suite d'un retard justifiable, sauf lorsque celui-ci est attribuable à l'omission du Canada de s'acquitter d'une de ses obligations en vertu du contrat.

7.12.11 Droit de résiliation

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

7.12.12 Services professionnels : Services de transition

(1) **Migration.** L'entrepreneur convient qu'en raison de la nature des services stipulés au contrat, le Canada peut exiger qu'ils soient fournis sans interruption. Avant la transition vers le nouveau l'entrepreneur ou au Canada, l'entrepreneur devra fournir toute l'information et la documentation opérationnelles, techniques, conceptuelles et configurationnelles nécessaires à la transition, dans la mesure où il ne s'agit pas de renseignements confidentiels d'entrepreneur (dont l'ensemble des données, de l'information et des éléments d'identification des utilisateurs du SAGU). L'entrepreneur déclare et certifie qu'il ne s'ingérera pas directement ou indirectement dans l'accès du Canada aux données du client ou leur transfert, ou qu'il n'y nuira pas directement ou indirectement.

- (2) **Services de migration et de transition.** L'entrepreneur convient que, durant la période menant à la fin du contrat, si des services de migration ou de transition sont demandés par le Canada, il aidera diligemment le Canada pendant la transition entre ce contrat et le nouveau contrat conclu avec le nouveau l'entrepreneur, ou pendant la migration des données du client vers un nouvel environnement de entrepreneur. De plus, les services ci-dessous ainsi assurés ne donneront lieu à aucun autre frais que ceux prévus dans la base de paiement.

7.12.13 Inspection et acceptation des travaux

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

7.13 Autorisation des tâches

- (1) **Autorisations de tâches au fur et à mesure des besoins.** La totalité ou une partie des travaux du contrat seront réalisés sur demande, au moyen d'une autorisation de tâches (AT). Les travaux décrits dans cette autorisation doivent être conformes à la portée du contrat. L'entrepreneur ne doit pas commencer les travaux avant d'avoir reçu une AT approuvée, émise par le Canada. L'entrepreneur convient que toute tâche effectuée avant la réception de cette autorisation de tâche approuvée est effectuée à ses propres risques.

(2) **Formulaire et contenu de l'ébauche de l'autorisation de tâches :**

- (a) Nous comprenons que le responsable technique des opérations transmettra à l'entrepreneur une description de la tâche à l'aide du formulaire d'autorisation de tâche.
- (b) L'ébauche de l'autorisation de tâche comprendra les détails des activités à exécuter, une description des produits livrables et un calendrier indiquant les dates d'achèvement des activités principales ou les dates de livraison des produits livrables. L'ébauche de l'autorisation de tâche comprendra aussi la base (les bases) et la méthode (les méthodes) de paiement prévues au contrat.
- (c) Une ébauche d'autorisation de tâche doit contenir les renseignements suivants, s'il y a lieu :
 - a. le numéro de la tâche;
 - b. la date à laquelle la réponse d'entrepreneur doit être reçue (cette date figurera sur l'ébauche de l'AT, mais pas sur l'AT attribuée);
 - c. le détail des codes financiers à utiliser;
 - d. les catégories de ressources et le nombre de ressources nécessaires;
 - e. une description des travaux associés à la tâche, portant sur les activités à réaliser ou indiquant les produits livrables (rapports, par exemple);
 - f. les dates de commencement et d'achèvement;
 - g. les dates jalons pour les produits livrables et les paiements (le cas échéant);
 - h. le nombre de jours-personnes requis;
 - i. une note à savoir si les travaux comprennent des activités à réaliser sur place, en précisant l'endroit;
 - j. le profil linguistique des ressources requises;
 - k. le niveau d'attestation de sécurité que doivent posséder les ressources;
 - l. le prix payable à l'entrepreneur pour l'exécution de la tâche, en indiquant s'il s'agit d'un prix ferme ou du prix maximum pour l'AT (et, pour les autorisations de tâche au prix maximum, l'AT doit indiquer la façon dont le montant final payable sera déterminé; lorsque l'AT n'indique pas la façon dont le montant final payable sera déterminé, le montant payable

est le montant, jusqu'à concurrence du montant maximum, pour les heures réellement travaillées sur le projet que l'entrepreneur justifie en présentant les feuilles de présence remplies au moment de l'exécution des travaux par les employés pour justifier les frais);

m. toute autre contrainte qui pourrait avoir des répercussions sur l'exécution de la tâche.

(3) **Réponse d'entrepreneur à l'ébauche de l'autorisation de tâches.** L'entrepreneur doit remettre au responsable technique, dans les dix jours ouvrables suivant la réception de l'ébauche de l'autorisation de hes (ou tout autre délai plus long précisé dans l'ébauche), le prix total qu'il propose pour réaliser la tâche ainsi qu'une ventilation de ce prix, établie en fonction de la base de paiement stipulée au contrat. L'entrepreneur doit préparer cette proposition en tenant compte des tarifs stipulés dans le contrat. L'entrepreneur ne sera pas payé pour la préparation ni la présentation d'une réponse, ni pour la transmission d'autres renseignements que nécessitent la préparation et l'attribution officielle de l'AT.

(4) **Limite des AT et pouvoirs relatifs à l'attribution d'AT**

Pour être attribuée de façon officielle, une AT doit porter les signatures suivantes :

(a) Toute AT dont la valeur, incluant les révisions, est inférieure ou égale à 25 000 \$ (y compris les taxes applicables) doit être signée par :

- a. le responsable technique des opérations;
- b. un représentant d'entrepreneur.

(b) Toute AT dont la valeur est supérieure à ce montant doit être signée par :

- a. le responsable technique des opérations;
- b. un représentant d'entrepreneur.
- c. l'autorité contractante.

(5) Toute AT qui ne porte pas les signatures requises n'a pas été émise de façon officielle par le Canada et n'est donc pas valide. Tous les travaux effectués par l'entrepreneur sans que celui-ci ait reçu une AT valide seront effectués à ses propres risques. L'entrepreneur doit aviser l'autorité contractante s'il reçoit une AT qui ne porte pas les signatures requises. Au moyen d'un avis écrit envoyé à l'entrepreneur, l'autorité contractante peut suspendre en tout temps le pouvoir du client d'attribuer des AT, ou réduire la valeur indiquée au point (A) ci-dessus. L'avis de suspension ou de réduction prend effet dès la réception.

(6) **Rapports d'utilisation périodique.** L'entrepreneur doit compiler et tenir à jour des données sur les services fournis au gouvernement fédéral, conformément à l'autorisation de tâches valides émises dans le cadre du contrat. Il doit également fournir ces données au Canada, conformément aux exigences en matière de rapports décrites ci-après. Si certaines données ne sont pas disponibles, la raison doit être indiquée dans le rapport. Si aucun service n'a été fourni pendant une période donnée, l'entrepreneur doit soumettre un rapport portant la mention « NÉANT ». Les données doivent être présentées tous les trimestres à l'autorité contractante. De temps à autre, l'autorité contractante peut aussi demander un rapport provisoire pendant une période de référence.

(7) Voici la répartition des trimestres :

- (a) 1^{er} trimestre : du 1^{er} avril au 30 juin;
- (b) 2^e trimestre : du 1^{er} juillet au 30 septembre;

- (c) 3^e trimestre : du 1^{er} octobre au 31 décembre;
 - (d) 4^e trimestre : du 1^{er} janvier au 31 mars.
- (8) Les données doivent être présentées à l'autorité contractante au plus tard 15 jours civils après la fin de la période visée.
- (9) Chaque rapport doit contenir les renseignements suivants pour chaque autorisation de tâches valide attribuée (dans leur version modifiée) :
- (a) le numéro de l'autorisation de tâches et le numéro de la version modifiée, le cas échéant;
 - (b) le nom, ou une brève description, de chaque autorisation de tâche;
 - (c) le nom et la catégorie de ressources de chaque ressource participant à l'exécution de l'autorisation de tâches, le cas échéant;
 - (d) le coût total estimatif indiqué dans l'autorisation de tâches valide de chaque tâche, taxes applicables en sus;
 - (e) le montant total dépensé jusqu'à présent, taxes applicables en sus, pour chaque tâche autorisée;
 - (f) les dates de début et d'achèvement de chaque AT;
 - (g) l'état d'avancement de chaque tâche autorisée, s'il y a lieu (p. ex. indiquer si les travaux sont en cours ou si le Canada a annulé ou a suspendu l'AT).
- (10) Chaque rapport doit également contenir les renseignements cumulatifs suivants pour chaque AT valide attribuée (dans leur version modifiée) :
- (a) le montant (taxes applicables en sus) précisé dans le contrat (selon la dernière modification, s'il y a lieu) qui correspond à la responsabilité totale du Canada envers l'entrepreneur pour toutes les AT approuvées;
 - (b) le montant total (taxes applicables en sus) dépensé jusqu'à présent pour chaque tâche attribuée de façon officielle.
- (11) **Regroupement d'autorisations de tâches pour des raisons administratives.** Le contrat peut être modifié à l'occasion afin de tenir compte de l'ensemble des autorisations de tâches valides émises à ce jour et de consigner les travaux réalisés dans le cadre de ces autorisations de tâches à des fins administratives.

7.14 Base de paiement

- (1) **Abonnement.** En ce qui concerne les services, y compris l'accès à la solution et son utilisation, la documentation sur la solution, les services de soutien et les services d'infrastructure de technologie de l'information accessoires et supplémentaires requis (tous les services décrits dans le présent contrat qui ne sont pas des travaux), le Canada doit payer les prix indiqués dans l'Annexe B – Base de Paiement.
- (2) **Services professionnels fournis dans le cadre d'une autorisation de tâches.** Pour les services professionnels demandés par le Canada, conformément à une autorisation de tâches attribuée de façon officielle, le Canada paiera à l'entrepreneur, en arriérés, le prix ferme établi dans l'autorisation de tâches selon les taux quotidiens fermes tout compris indiqués dans l'Annexe B – Base de Paiement du contrat. Les taxes applicables sont en sus.
- (3) **Frais de soutien sur place.** Si le Canada l'approuve à l'avance, l'entrepreneur recevra les taux de main-d'œuvre horaires ou quotidiens précisés dans l'Annexe B – Base de Paiement du contrat, ainsi que les frais de déplacement et de subsistance raisonnables et appropriés engagés par l'entrepreneur dans le cadre des services sur place. Les frais de déplacement et de subsistance ne seront remboursés que conformément aux indemnités de repas et de véhicule particulier prévues dans la Directive sur les voyages du Conseil national mixte, telle que modifiée de temps à autre. Tous ces frais préapprouvés devront être facturés au Canada comme frais distincts.

7.15 Paiement

7.15.1 Factures

(1) **Présentation des factures.** L'entrepreneur doit présenter des factures, au besoin.

(2) **Exigences relatives à la facture.** Les factures doivent être au nom d'entrepreneur et contenir :

- (a) la date, le nom et l'adresse du ministère client, les numéros d'articles ou de référence, les produits livrables et la description du service ou des travaux, le numéro du contrat, le numéro de référence du client (NRC), le numéro d'entreprise - approvisionnement (NEA) et les codes financiers;
- (b) des renseignements sur les dépenses (comme le nom des articles et leur quantité, l'unité de distribution, le prix unitaire, les tarifs horaires fermes, le niveau d'effort et les sous-traitances, selon le cas) conformément à la base de paiement, excluant les taxes applicables;
- (c) les taxes applicables doivent être indiquées séparément dans toutes les factures, ainsi que les numéros d'inscription correspondants émis par les autorités fiscales. Tous les articles détaxés, exonérés ou auxquels les taxes applicables ne s'appliquent pas doivent être identifiés comme tels sur toutes les factures.
- (d) les déductions correspondant à la retenue de garantie, s'il y a lieu;
- (e) les prix totaux calculés, le cas échéant.

7.15.2 Taxes

- (1) **Paiement des taxes.** Les taxes applicables seront payées par le Canada conformément aux dispositions de l'article sur la présentation des factures. Il revient à l'entrepreneur de facturer les taxes applicables selon le taux approprié, conformément aux lois en vigueur. L'entrepreneur accepte de remettre aux autorités fiscales concernées le montant de taxes applicables versées ou exigibles.
- (2) **Retenue pour les non-résidents.** Le Canada doit retenir 15 % du montant à payer à l'entrepreneur pour des services rendus au Canada si l'entrepreneur n'est pas un résident du Canada, à moins que ce dernier obtienne une exonération valide de l'Agence du revenu du Canada. Le montant retenu sera conservé dans un compte pour l'entrepreneur à l'égard de toute dette fiscale exigible par le Canada.
- (3) **Attestation de factures.** En présentant une facture, l'entrepreneur atteste que les produits et services ont été livrés et que tous les frais sont conformes aux dispositions du contrat.

7.15.3 Période de paiement

Le Canada paiera le montant non contesté de la facture d'entrepreneur dans les 30 jours suivant sa réception. Dans l'éventualité où une facture n'est pas dans une forme et un contenu acceptables, le Canada en avisera l'entrepreneur et le délai de paiement de 30 jours débutera à la réception d'une facture conforme.

7.15.4 Intérêts sur les paiements en retard

Le Canada versera à l'entrepreneur des intérêts simples, au taux moyen majoré de 3 % par an, sur toute somme en souffrance, à partir du premier jour où la somme est en souffrance jusqu'au jour qui précède la date de paiement inclusivement, à condition que le Canada soit responsable du retard de paiement à l'entrepreneur. Le Canada ne versera pas d'intérêts sur les paiements anticipés qui sont en souffrance.

7.15.5 Modalités de paiement

Le Canada paiera pour les services prévus au contrat, soit à l'avance, soit à terme échu, conformément à l'annexe F, Accords sur les niveaux de service du logiciel-service, ou à la soumission d'entrepreneur, le cas échéant. Lorsque le paiement est effectué à l'avance, la période de

paiement anticipé ne dépasse pas 12 mois. Le paiement anticipé n'empêche pas le Canada d'exercer un recours à l'égard de ce paiement ou de la prestation des services.

Si le Canada conteste une facture pour quelque raison que ce soit, il réglera à l'entrepreneur la tranche de la facture non contestée, à la condition que les articles non contestés soient indiqués distinctement sur la facture et que leur paiement soit exigible. Dans le cas des factures contestées, elles ne seront réputées reçues qu'une fois le litige réglé.

7.15.6 Limitation des dépenses

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

7.15.7 Paiement électronique des factures

L'entrepreneur accepte d'être payé au moyen de l'un des instruments de paiement électronique suivants :

- (1) Carte d'achat Visa;
- (2) Carte d'achat MasterCard;
- (3) Dépôt direct (national et international);
- (4) Échange de données informatisé (EDI);
- (5) Virement télégraphique (international seulement);
- (6) Système de transfert de paiements de grande valeur (plus de 25 M\$).

7.15.8 Exigences en matière d'assurances

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

7.16 Stabilité des Prix

L'entrepreneur reconnaît qu'il est important pour le Canada de pouvoir continuer à accéder aux produits et services ANS décrits dans le contrat. En conséquence, le contractant propose de continuer à fournir les produits et services ANS à des tarifs raisonnables et selon toutes les autres conditions générales énoncées dans le présent contrat, sous réserve de l'exécution par les parties d'un ou de plusieurs contrats formels à cet effet. Pour chacune des 2 années qui suivent la durée du contrat, l'entrepreneur offre par la présente des taux annuels qui sont le moindre des montants suivants:

- a) les tarifs alors en vigueur publiés par l'entrepreneur; et
 - b) es taux précédemment contractés ajustés de la différence en pourcentage de l'indice des prix à la consommation (IPC) tel que déterminé par Statistique Canada, pour la période de 12 mois précédant immédiatement la date à laquelle la modification des prix doit entrer en vigueur; et
 - c) 3% de plus que les taux annuels fournis au Canada au cours de l'année précédente en vertu du présent contrat ou de toute prolongation conclue conformément au présent article;
- et les obligations de l'entrepreneur en vertu du présent article survivront à la résiliation ou à l'expiration du présent contrat.

7.17 Certification des Prix

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

7.18 LIMITATION DE RESPONSABILITÉ

7.18.1 Responsabilité de première partie

7.18.1.1 **Exécution du contrat** : L'entrepreneur est entièrement responsable de tous les dommages subis par le Canada, causés par l'exécution ou l'inexécution du contrat par l'entrepreneur.

7.18.1.2 **Fuite de données** : L'entrepreneur est entièrement responsable de tous les dommages subis par le Canada, causés par une infraction à la sécurité ou un manquement à l'obligation de confidentialité entraînant la consultation ou la divulgation non autorisées de dossiers, de données ou de renseignements appartenant au Canada ou à un tiers.

7.18.1.3 **Limitation par incident** : Sous réserve de la clause suivante, quel que soit le fondement ou la nature de la réclamation, la responsabilité totale par incident de l'entrepreneur n'excédera pas la valeur cumulative des factures liées au contrat au cours des douze (12) mois précédant l'incident.

7.18.1.4 **Aucune limitation** : La limitation de responsabilité susmentionnée de l'entrepreneur ne s'applique pas :

- a) à toute in conduite volontaire ou à tout acte répréhensible délibéré;
- b) à tout manquement aux obligations relatives à la garantie.

7.18.2 Responsabilité de tierce partie : Chaque partie convient qu'elle est pleinement responsable des dommages qu'elle cause à un tiers dans le cadre du contrat, que la réclamation soit déposée par le tiers auprès du Canada ou de l'entrepreneur, ou des deux. Le montant de la responsabilité sera celui précisé dans l'accord conclu entre les parties ou déterminé par la cour. Les parties conviennent de se rembourser mutuellement tout paiement versé à un tiers en lien avec les dommages causés par l'autre partie et de rembourser rapidement leur part de responsabilité.

7.19 Dispositions générales

(1) **Lois applicables.** Le présent contrat sera interprété et régi selon les lois en vigueur en _____.

(À remplir au moment de l'attribution du contrat à l'aide de l'information issue de la soumission.)

(2) **Survie.** Les obligations des parties concernant la confidentialité, les déclarations et les garanties prévues dans le contrat ainsi que les dispositions qu'il est raisonnable de présumer, en raison de la nature des droits et des obligations, qu'elles devraient rester en vigueur, demeurent applicables malgré l'expiration du contrat ou sa résiliation.

(3) **Divisibilité.** Si une disposition du contrat est déclarée non exécutoire par un tribunal faisant autorité, le reste du contrat restera en vigueur.

(4) **Renonciation.** L'échec ou la négligence d'une partie de faire respecter l'un des droits en vertu du contrat ne seront pas considérés comme une renonciation des droits de cette partie.

(5) **Aucun pot-de-vin.** L'entrepreneur déclare qu'aucun pot-de-vin, cadeau, bénéfice ou autre avantage n'a été ni ne sera payé, donné, promis ou offert, directement ou indirectement, à un représentant ou à un employé du Canada ni à un membre de sa famille, en vue d'exercer une influence sur l'attribution ou la gestion du contrat.

(6) **Honoraires conditionnels.** L'entrepreneur atteste qu'il n'a pas versé ni convenu de verser, directement ou indirectement, et convient de ne pas verser, directement ou indirectement, des honoraires conditionnels en rapport avec la soumission, la négociation ou l'obtention du contrat à toute personne autre qu'un employé d'entrepreneur remplissant les fonctions habituelles liées à son poste. Dans le présent article, « honoraires conditionnels » signifie tout paiement ou autre forme de rémunération qui est subordonnée au degré de succès ou calculée en fonction du degré de succès obtenu dans la sollicitation, la négociation ou l'obtention du contrat et « personne » signifie tout particulier qui est tenu de fournir au registraire une déclaration en vertu de l'article 5 de la *Loi sur le lobbying*, 1985, c. 44 (4^e supplément).

(7) Sanctions internationales

(a) Les personnes au Canada et les Canadiens et les Canadiennes à l'étranger sont liés par les sanctions économiques imposées par le Canada. Par conséquent, le gouvernement du Canada ne peut accepter la livraison d'aucun bien ou la prestation d'aucun service provenant, directement ou indirectement, de personnes ou de pays assujettis aux sanctions économiques.

(b) L'entrepreneur ne doit pas fournir au gouvernement du Canada un bien ou un service assujetti à des sanctions économiques.

(c) L'entrepreneur doit se conformer aux modifications apportées au règlement imposé pendant la période du contrat. L'entrepreneur doit immédiatement aviser le Canada s'il est dans l'impossibilité d'exécuter le contrat parce qu'on a imposé des sanctions à un pays ou à une personne ou qu'on a ajouté des biens ou des services à la liste des biens ou des services sanctionnés. Si les parties ne peuvent alors s'entendre sur un plan de redressement, le contrat sera résilié.

(8) **Dispositions relatives à l'intégrité – Contrat.** La Politique d'inadmissibilité et de suspension (la « Politique ») et toutes les directives incorporées par renvoi à la demande de soumissions à sa date de clôture sont intégrées au contrat et en font partie intégrante.

L'entrepreneur doit se conformer aux dispositions de la politique et des directives; celles-ci se trouvent sur le site Internet de Travaux publics et Services gouvernementaux Canada sous Politique d'inadmissibilité et de suspension.

(9) **Code de conduite pour l'approvisionnement – Contrat.** L'entrepreneur accepte de se conformer au Code de conduite de l'approvisionnement et d'être lié par celui-ci pendant la durée du contrat.

(10) **Code régissant les conflits d'intérêts et code de valeurs et d'éthique de la fonction publique.** L'entrepreneur reconnaît que les personnes qui sont assujetties aux dispositions de la *Loi sur les conflits d'intérêts* 2006, ch. 9, art. 2, du *Code régissant la conduite des titulaires de charge publique* en ce qui concerne les conflits d'intérêts et l'après-mandat, du *Code de valeurs et d'éthique de la fonction publique* ou tout autre code de valeur et d'éthique en vigueur au sein d'organismes spécifiques ne peuvent bénéficier directement du contrat.

(11) Responsables

(a) Autorité contractante

Nom : Daniel Ferguson
Titre : Chef d'équipe d'approvisionnement
Téléphone : 343-543-3961
Courriel : daniel.ferguson@tpsgc-pwgsc.gc.ca

L'autorité contractante doit recevoir une copie de la facture pour le dossier et l'examen du Canada.

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

(b) Responsable technique des opérations

Nom : Jennifer Forsythe
Titre : Gestionnaire, Gestion des urgences et continuité des opérations
Téléphone : 819-654-4672
Courriel : jennifer.forsythe@servicecanada.gc.ca

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

(c) Personne-ressource pour les questions administratives

Nom : Jennifer Forsythe
Titre : Gestionnaire, Gestion des urgences et continuité des opérations
Téléphone : 819-654-4672
Adresse courriel : Jennifer.forsythe@servicecanada.gc.ca

(d) Autorité de Sécurité de la Chaîne d'Approvisionnement

Nom :
Titre :
Téléphone :
Adresse courriel :

L'autorité de sécurité de la chaîne d'approvisionnement est le représentant de Services partagés Canada (SPC) et elle est responsable de toutes les questions liées au processus continu d'intégrité de la chaîne d'approvisionnement en vertu du présent contrat. Ni l'autorité contractante ni l'autorité technique n'ont le pouvoir de fournir des conseils ou d'autoriser la divulgation de renseignements liés au processus d'intégrité de la chaîne d'approvisionnement. L'autorité contractante demeure responsable de tous les autres aspects liés à la sécurité.

7.20 Obligations en matière de sécurité

7.20.1 Objet

La présente annexe a pour objet d'énoncer les obligations d'entrepreneur relativement à la configuration et à la gestion appropriées des biens et des actifs d'information, afin de protéger ces biens et actifs d'information contre toute modification, accès ou exfiltration non autorisés, le tout conformément au contrat, à la présente annexe, aux mesures de sécurité particulières d'entrepreneur et aux politiques du Canada sur la sécurité (collectivement, les « obligations de sécurité »).

7.20.2 Transfert des obligations en matière de sécurité

Les obligations d'entrepreneur contenues dans les présentes Obligations de sécurité doivent être transférées par l'entrepreneur aux Sous-traitants d'entrepreneur, dans la mesure applicable à chaque Sous-traitant d'entrepreneur, étant donné la nature des services qu'il fournit à l'entrepreneur.

7.20.3 Reconnaissances

(1) Les parties reconnaissent que :

- (a) Tous les biens et les actifs informationnels sont assujettis à ces obligations en matière 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 biens et aux actifs d'information.
- (c) L'entrepreneur ne doit pas avoir ou tenter d'obtenir la garde d'un actif d'information, ni permettre à un membre du personnel des services d'accéder à un actif d'information avant la mise en œuvre des exigences en matière de sécurité, comme l'exige la présente annexe, au plus tard à l'attribution du marché.

7.20.4 Protection des actifs d'information

L'entrepreneur doit concevoir ses services de manière à protéger les biens et les actifs d'information contre tout accès, modification ou exfiltration non autorisés. Cela comprend la mise en œuvre et le maintien de politiques, de procédures et de contrôles de sécurité de l'information appropriés afin de préserver la confidentialité, l'intégrité et la disponibilité des biens et des actifs d'information (ci-après appelés les « mesures de sécurité particulières »).

7.20.5 Rôles et responsabilités liés à la mise en œuvre

- (1) L'entrepreneur doit s'assurer que les rôles et responsabilités relatifs aux contrôles et aux fonctions de sécurité des services sont clairement définis pour lui-même et pour le Canada. Cela comprend, à tout le moins, les rôles et les responsabilités des parties pour : i) la gestion des comptes; ii) la protection des frontières; iii) la sauvegarde des actifs et des systèmes d'information; iv) la gestion des incidents; v) la surveillance du système; et vi) la gestion de la vulnérabilité.
- (2) L'entrepreneur doit fournir au Canada un document à jour qui définit les rôles et les responsabilités d'entrepreneur, des sous-traitants d'entrepreneur et du Canada en matière de contrôles et de caractéristiques de sécurité : i) annuellement; ii) lorsqu'il y a des changements importants à ces rôles et responsabilités à la suite d'un changement aux services; ou iii) à la demande du Canada.

7.20.6 Assurance tierce : certifications et rapports

- (1) L'entrepreneur doit prouver sa conformité aux certifications et aux rapports d'audit suivants en présentant des rapports d'évaluation ou des certifications de tierce partie indépendante pour toutes les parties du service :
- (2) Chaque certification ou rapport d'audit présenté doit : i) déterminer la raison sociale légale d'entrepreneur ou du sous-traitant d'entrepreneur concerné; ii) déterminer la date de certification d'entrepreneur ou du sous-traitant d'entrepreneur; iii) déterminer la liste

des biens, des infrastructures d'entrepreneur et des emplacements du service dans le cadre du rapport de certification. Si la méthode créée est utilisée pour exclure les organisations de sous-services comme la prise en charge de centres de données, le rapport d'évaluation de l'organisation de sous-services doit être joint.

- (3) Chaque certification ISO fournie doit être valide pendant toute la durée du contrat, dans les 12 mois précédant le début du contrat. Les certifications doivent être accompagnées de preuves à l'appui, comme le rapport d'évaluation ISO élaboré pour valider la conformité à la certification ISO.

- (4) Chaque rapport d'audit SOC doit avoir été réalisé dans les 12 mois précédant le début du contrat.

- (5) L'entrepreneur doit maintenir la validité de sa certification selon les normes décrites au paragraphe 5(1) pendant toute la durée du contrat. L'entrepreneur doit fournir, au moins une fois par année, et sans délai à la demande du Canada, tous les rapports ou dossiers qui peuvent être raisonnablement requis pour démontrer que les certifications d'entrepreneur demeurent à jour et sont valides pour la durée du contrat.

7.20.7 Audit de conformité

- (1) L'entrepreneur doit effectuer les vérifications de confidentialité et de sécurité de la sécurité des ordinateurs, de l'environnement informatique et des centres de données physiques qu'il utilise pour traiter et protéger les biens et les actifs d'information, comme suit :

- (a) Lorsqu'une norme ou un cadre prévoit des vérifications, une vérification de cette norme ou de ce cadre de contrôle sera entreprise au moins une fois par année;
- (b) Chaque audit sera effectué conformément aux normes et règles de l'organisme de réglementation ou d'accréditation pour chaque norme ou cadre de contrôle applicable;
- (c) Chaque vérification sera effectuée par un vérificateur tiers qualifié et 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 17 020 sur les systèmes de management de la qualité à la sélection et aux frais d'entrepreneur.

- (2) Chaque audit donnera lieu à la production d'un rapport d'audit qui doit être communiqué au Canada. Le rapport de vérification doit indiquer clairement toutes les constatations importantes faites par le vérificateur externe. L'entrepreneur doit corriger rapidement et à la satisfaction du vérificateur les problèmes soulevés dans tout rapport de vérification et doit (i) fournir au Canada le plan pour corriger toute constatation négative découlant de ces rapports et (ii) fournir au Canada, sur demande, des rapports d'étape sur la mise en œuvre dans les dix (10) jours ouvrables du gouvernement fédéral.

7.20.8 Protection cryptographique

- (1) L'entrepreneur doit :

- (a) Mettre en œuvre le chiffrement des données au repos pour tous les actifs d'information;
- (b) Prendre des mesures raisonnables pour s'assurer que le chiffrement des données au repos demeure en vigueur, ininterrompu et actif en tout temps, même en cas de panne d'équipement ou de technologie;
- (c) Transmettre les actifs d'information de manière sécuritaire; Cela comprend la mise en œuvre du chiffrement des données en transit pour toutes les transmissions de biens et d'actifs d'information;

- (d) L'entrepreneur ne doit pas faire de copies des bases de données ou de toute partie de ces bases de données contenant des actifs d'information et ne doit pas déplacer ou transmettre des copies approuvées à quelque endroit que ce soit, sauf lorsque l'approbation du Canada est obtenue.

7.20.9 Séparation des données

- (1) L'entrepreneur doit mettre en place des contrôles afin d'assurer un isolement approprié des ressources, afin que les actifs d'information ne se retrouvent pas mêlés aux données d'autres locataires, et ce, pendant l'utilisation, le stockage ou le transfert, et dans tous les aspects des fonctions et de l'administration du système du service et de l'infrastructure d'entrepreneur. Cela comprend la mise en œuvre de contrôles d'accès et la mise en place d'une séparation logique ou physique appropriée pour soutenir :
- (a) la séparation de l'administration interne d'entrepreneur des ressources utilisées par ses clients; et
 - (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.

7.20.10 Emplacement des données et isolement aux fins de protection

- (1) La solution de logiciel-service doit permettre au Canada de stocker et de protéger ses actifs d'information, en transit ou inactifs, 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 est défini comme suit :
- (a) Un centre de données qui répond à toutes les exigences et certifications de sécurité identifiées à la section 29 pour les centres de données et installations (c.-à-d. la sécurité physique).
 - (b) Emploie un chiffrement par algorithmes cryptographiques approuvés par le CSTC pour voir à ce qu'aucune donnée ne soit gravée sur disque sous une forme non chiffrée : <https://www.cse-cst.gc.ca/fr/publication/itsa-11e>.
- (2) L'entrepreneur doit attester que la prestation et l'approvisionnement des services en vertu du présent marché proviennent de pays membres de l'Organisation du traité de l'Atlantique Nord (OTAN) (https://www.nato.int/cps/fr/natohq/nato_countries.htm) ou de l'Union européenne (UE) (https://europa.eu/european-union/about-eu/countries_fr), ou encore de pays avec lesquels le Canada a conclu un instrument international bilatéral de sécurité industrielle. Dans le cadre du Programme de sécurité des contrats, des accords internationaux bilatéraux en matière de sécurité industrielle ont été conclus avec les pays énumérés sur le site Web <https://www.tpsgc-pwgsc.gc.ca/esc-src/international-fra.html> de SPAC, tel qu'il est mis à jour de temps à autre.

7.20.11 Protection des données

- (1) L'entrepreneur doit permettre au Canada d'isoler les biens et les actifs d'information dans des centres de données situés géographiquement au Canada.
- (2) Garantit l'impossibilité de trouver les données d'un client en particulier sur des supports physiques; et
- (3) Sur demande, l'entrepreneur doit :
- (a) Fournir au GC une liste à jour des emplacements physiques, y compris la ville, qui peuvent contenir les biens et les actifs d'information pour chaque centre de données qui sera utilisé pour fournir les services; et
 - (b) avisant expressément le Canada de l'intention future du fournisseur d'utiliser des services tiers ou API dans le cadre du service qui pourrait être fourni, de l'extérieur du Canada, en précisant tous ces emplacements à l'étranger (pays, province, ville) où les données seraient stockées et traitées et d'où ils gèrent le service, afin que le Canada prenne la décision appropriée d'accepter ou non cette modification.

- (4) L'entrepreneur des Services proposés a l'obligation continue d'aviser le Canada lorsqu'il y a des mises à jour de la liste des emplacements physiques qui peuvent contenir des biens et des actifs d'information.

7.20.12 Transfert et récupération des données

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

- (a) Extraire tous les actifs d'information en ligne, pseudo-directs et hors-ligne, y compris, sans toutefois s'y limiter, les bases de données, le stockage d'objets et de fichiers, les configurations de système, les journaux d'activités infonuagiques, de sorte que tout utilisateur final du Canada puisse se servir de ces instructions pour effectuer la migration d'un environnement à un autre;
- (b) Effectuer le transfert sécurisé de tous les actifs d'information, y compris les métadonnées, dans un format lisible et utilisable par machine acceptable pour le Canada, conformément aux *Lignes directrices sur les formats de fichier à utiliser pour transférer des ressources documentaires* de Bibliothèque et Archives Canada (<https://www.bac-lac.gc.ca/fra/services/gestion-ressources-documentaires-gouvernement/lignes-directrices/Pages/lignes-directrices-formats-fichier-transferts-ressources-documentaires.aspx>).

7.20.13 Élimination de données et retour d'archives au Canada.

- (1) En cas de résiliation ou d'expiration du contrat, l'entrepreneur doit retourner toutes les données du gouvernement du Canada conformément au critère O45 de l'énoncé des besoins.
- (2) L'entrepreneur doit, sur demande, éliminer ou réutiliser en toute sécurité les ressources (p. ex. l'équipement, le stockage des données, les fichiers et la mémoire) qui contiennent des actifs d'information et voir à ce que les données précédemment stockées ne peuvent être traitées par d'autres clients après leur diffusion. Cela concerne toutes les copies des actifs d'information du Canada qui sont créées pour permettre une disponibilité accrue et une reprise après sinistre. L'élimination ou la réutilisation des ressources par l'entrepreneur doit être harmonisée à l'un des documents suivants : (i) Manuel d'utilisation du Programme national de sécurité industrielle (DoD 5220.22-M6); (ii) Lignes directrices pour l'assainissement des supports (NIST SP 800-88); ou (iii) Effacement et déclassification des supports d'information électroniques (CSTC ITSG-06).
- (3) L'entrepreneur doit fournir des preuves démontrant qu'il a réussi à effacer, à purger ou à détruire toutes les ressources, selon le cas, et qu'il est en mesure d'empêcher le rétablissement de tout système, de toute capacité (logiciel ou processus), de toute donnée ou de toute information retirés ou détruits après leur retrait de l'instance du Canada.

7.20.14 Contrôle de l'accès

- (1) L'entrepreneur doit avoir la capacité pour le Canada de soutenir un accès sécurisé aux services, y compris la capacité de configurer :
- (a) Une authentification à facteurs multiples conformément au document ITSP.30.031 V2 (ou une version subséquente) du CST (<https://www.cse-cst.gc.ca/fr/node/1842/html/26717>) au moyen de justificatifs approuvés par le GC;
 - (b) Un accès en fonction du rôle;
 - (c) Les contrôles d'accès aux objets entreposés;
 - (d) Les politiques d'autorisation granulaire pour permettre ou limiter l'accès; et
 - (e) De mettre en œuvre des contrôles de sécurité qui restreignent l'accès administratif d'entrepreneur aux actifs et aux systèmes d'information et lui permettent d'exiger l'approbation du Canada avant que l'entrepreneur puisse avoir accès aux actifs d'information pour effectuer des activités opérationnelles, de soutien ou de maintenance en utilisant des actifs d'information qui comprennent des données canadiennes;

- (f) De prendre des mesures raisonnables pour s'assurer que le personnel des Services n'a pas de droits d'accès permanents ou continus aux actifs d'information, et l'accès est limité à ceux qui doivent avoir accès aux biens et aux actifs d'information pour fournir un soutien technique ou à la clientèle, sur approbation du Canada.

7.20.15 Fédération de l'identité

- (1) L'entrepreneur doit permettre au Canada de soutenir l'intégration de l'identité fédérée. Pour ce faire, il doit notamment :
 - (a) Mettre en œuvre des mécanismes d'authentification multifactorielle pour authentifier les utilisateurs finaux ayant un accès privilégié, conformément à la norme ITSP.30.031 V2 du CCC (ou à ses versions ultérieures);
 - (b) Prendre en charge le Security Assertion Markup Language (SAML) 2.0 et OpenID Connect 1.0, où les justificatifs et authenticateurs des utilisateurs finaux pour les services d'infonuagique sont contrôlés uniquement par le Canada;
 - (c) Associer les identifiants uniques du Canada (p. ex. un numéro d'identification unique du Canada, une adresse de courriel du Canada) aux comptes d'utilisateurs des services d'infonuagique correspondants.

7.20.16 Protection des points terminaux

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

7.20.17 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, 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.

7.20.18 Interface de programmation d'applications

(1) L'entrepreneur doit :

- (a) Rendre des services qui utilisent des interfaces de programmation d'applications (API) ouvertes, publiées, prises en charge et documentées pour prendre en charge l'interopérabilité entre les composants et faciliter la migration des applications.
- (b) Prendre des mesures raisonnables pour protéger les API internes et externes grâce à des méthodes d'authentification sécurisées, notamment de voir à ce que toutes les requêtes API exposées à l'externe nécessitent une authentification réussie avant qu'elles puissent être appelées.

(2) Pour le ANS, l'entrepreneur doit fournir des API qui permettent :

- (a) D'interroger les données au repos dans les applications ANS; et
- (b) D'évaluer les événements et les incidents stockés dans les journaux des applications ANS.

7.20.19 Gestion de l'accès privilégié

(1) L'entrepreneur doit :

- (a) Gérer et surveiller l'accès privilégié aux services infonuagiques pour s'assurer que toutes les interfaces de service dans un environnement à locataires multiples sont protégées contre tout accès non autorisé, y compris celles qui sont utilisées pour héberger les services du GC;
- (b) Restreindre et minimiser l'accès aux services et aux actifs d'information du Canada seulement aux appareils autorisés et aux utilisateurs finaux ayant explicitement besoin de cet accès;
- (c) Appliquer et vérifier les autorisations d'accès aux services et aux actifs d'information;
- (d) Confiner tous les accès aux interfaces de service qui hébergent les biens et les actifs d'information à des utilisateurs finaux, des dispositifs et des processus (ou des services) identifiés, authentifiés et autorisés de manière unique;
- (e) Mettre en œuvre des politiques sur les mots de passe afin de protéger les justificatifs d'identité contre les attaques en ligne ou hors ligne et de détecter ces attaques en consignait et en surveillant des événements tels que (i) l'utilisation réussie des justificatifs d'identité, (ii) l'utilisation inhabituelle de ces derniers et (iii) l'accès et l'exfiltration de la base de données des mots de passe, conformément à la version 2 (ou aux versions ultérieures) des Normes ITSP.30.031 du CST (<https://cyber.gc.ca/en/publications/html/26717>);
- (f) Mettre en œuvre des mécanismes d'authentification multifactorielle pour authentifier les utilisateurs finaux ayant un accès privilégié, conformément à la norme ITSP.30.031 V2 (ou versions ultérieures) du CST (<https://www.cse-cst.gc.ca/fr/node/1842/html/26717>);
- (g) Mettre en place des contrôles de l'accès fondés sur le rôle qui forment la base de l'accès aux biens et aux actifs d'information;

- (h) Définir et mettre en œuvre la séparation des tâches pour, au minimum, séparer les rôles de gestion des services et d'administration des rôles de soutien du système d'information, les rôles de développement des rôles opérationnels et les rôles de gestion de l'accès des autres rôles opérationnels;
- (i) Adhérer aux principes du moindre privilège et du besoin de savoir pour accorder l'accès aux services et aux biens et aux actifs d'information;
- (j) Utiliser des points terminaux à sécurité élevée (ordinateurs, appareils d'utilisateurs finaux, serveurs intermédiaires, etc.) qui sont configurés de façon à offrir seulement des fonctions minimales (par exemple un point terminal dédié qui ne peut pas être utilisé pour naviguer sur Internet ou consulter ses courriels) pour offrir le soutien et l'administration des services et de l'infrastructure d'entrepreneur;
- (k) 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;
- (l) Révoquer, en cas de cessation d'emploi, les authentifiant et les justificatifs d'accès associés à tout personnel de services.

7.20.20 Gestion à distance d'entrepreneur

- (1) L'entrepreneur doit gérer et surveiller l'administration à distance des services d'entrepreneur 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 V2 (ou versions ultérieures) du CST (<https://www.cse-cst.gc.ca/fr/node/1842/html/26717>);
 - (b) Employer un algorithme cryptographique approuvé par le CSTC pour protéger la confidentialité des séances d'accès à distance : <https://www.cse-cst.gc.ca/en/publication/itsa-11e>;
 - (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.

7.20.21 Sécurité des réseaux et des communications

- (1) L'entrepreneur doit :
 - (a) Permettre au Canada d'établir des connexions sécurisées aux Services, notamment en assurant la protection des données en transit entre le Canada et le Service au moyen de TLS 1.2 ou de versions ultérieures, et en utilisant des algorithmes et des certificats cryptographiques pris en charge, comme le décrit les normes ITSP.40.062 (<https://cyber.gc.ca/fr/orientation/conseils-sur-la-configuration-securisee-des-protocoles-reseau-itsp40062>) et ITSP.40.111 (<https://cyber.gc.ca/fr/orientation/algorithmes-cryptographiques-pour-linformation-non-classifie-protège-et-protège-b>) du CST;
 - (b) Offrir une protection des données en transit entre les microservices et les applications utilisées au sein des Services;
 - (c) Utiliser des certificats correctement configurés dans les connexions TLS conformément aux directives du CST;
 - (d) Désactiver les protocoles vulnérables connus, comme toutes les versions de Secure Sockets Layer (SSL) (p. ex. SSLv2 et SSLv3) et toutes les versions antérieures de TLS (p. ex. TLS 1.0 et TLS 1.1), conformément à la norme ITSP.40.062 du CST, ainsi que les modes de chiffrement vulnérables connus (p. ex. RC4 et 3DES);

- (e) Permettre au Canada de mettre en œuvre des contrôles d'accès au réseau et des règles de sécurité qui permettent ou refusent le trafic réseau vers les ressources canadiennes.

7.20.22 Accès et vérification

- (1) L'entrepreneur doit mettre en œuvre des pratiques et des contrôles de production et de gestion de journaux pour toutes les composantes du service qui stockent ou traitent les biens et les actifs d'information, et qui sont conformes aux pratiques des principaux entrepreneurs de services, comme celles de NIST 800-92 (Guide to Computer Security Log Management), ou une norme équivalente approuvée par écrit par le Canada.
- (2) L'entrepreneur doit tenir un registre des problèmes signalés (dossiers d'incident) avec au moins les données suivantes (nom du déclarant ou du demandeur, description de la résolution, nombre de problèmes nécessitant un acheminement, délai d'exécution estimé de la résolution).
- (3) L'entrepreneur doit permettre au Canada d'examiner et d'analyser de manière centralisée les dossiers de vérification de multiples composants des services offerts par l'entrepreneur. Ceci comprend la capacité du Canada :
 - (a) D'enregistrer et de détecter les événements de vérification tels qu'un minimum (i) de tentatives de connexion réussies ou non, (ii) de gestion des comptes, (iii) d'accès aux objets et changement de politique, (iv) de fonctions de privilèges et de suivi des processus, (v) d'événements système, (vi) de suppression des données;
 - (b) D'enregistrer dans des journaux (ou fichiers journaux) des événements de vérification qui sont synchronisés et horodatés en temps universel coordonné (UTC) et protégés contre l'accès, la modification ou la suppression non autorisée, que ces données soient en transit ou inactives;
 - (c) De repérer des incidents de sécurité et des journaux de bord distincts pour les différents comptes du Canada afin de permettre au GC de surveiller et de gérer les événements à l'intérieur de ses frontières qui ont une incidence sur l'instance d'un service IaaS, PaaS ou SaaS qui lui est rendu par l'entrepreneur ou un sous-traitant d'entrepreneur;
 - (d) De transmettre les événements et journaux des locataires du Canada vers un système centralisé de journaux de vérification géré par le GC au moyen d'interfaces d'établissement de rapports, de protocoles et de formats de données (Common Event Format [CEF], Syslog et autres formats communs) et d'interface de programmation d'application normalisés qui permettent la récupération à distance des données de journaux (par l'intermédiaire d'une interface de base de données qui utilise SQL, etc.).

7.20.23 Surveillance continue

- (1) L'entrepreneur doit continuellement gérer, surveiller et maintenir la posture de sécurité de tous les biens, de l'infrastructure d'entrepreneur et des emplacements de service pendant toute la durée du contrat, et s'assurer que les services fournis au Canada sont conformes aux présentes obligations en matière de sécurité. Dans le cadre de l'obligation, l'entrepreneur doit :
 - (a) Surveiller activement et continuellement les menaces et les vulnérabilités pesant sur les actifs, l'infrastructure d'entrepreneur, les emplacements de service ou les actifs d'information;
 - (b) Faire de son mieux pour prévenir les attaques au moyen de mesures de sécurité comme les protections contre le refus de service;
 - (c) Faire de son mieux pour détecter les attaques, les incidents de sécurité et autres événements anormaux;
 - (d) Détecter l'utilisation et l'accès non autorisés à tous les services, données et composants pertinents aux services IaaS, PaaS ou SaaS du Canada;

- (e) Gérer et appliquer les correctifs et les mises à jour liés à la sécurité de manière opportune et systématique afin d'atténuer les vulnérabilités et de remédier à tout problème signalé publiquement dans les services ou les bibliothèques que les services utilisent, et fournir des avis préalables liés aux correctifs conformément aux engagements convenus relatifs au niveau de service;
 - (f) Répondre aux menaces et aux attaques contre les services d'entrepreneur, les contenir et veiller à la récupération;
 - (g) Au besoin, prendre des contre-mesures proactives, y compris, des mesures préventives et d'intervention permettant d'atténuer les menaces.
- (2) Les services d'entrepreneur doivent permettre de copier les données des applications (IaaS, PaaS et ANS) et le trafic réseau (IaaS et PaaS) du gouvernement du Canada dans les services informatiques hébergés et de les acheminer vers un emplacement prédéterminé (dans le nuage ou dans les locaux du gouvernement).
- (3) Les services d'entrepreneur doivent permettre au Canada de déployer et d'utiliser des logiciels de sécurité pour assurer la surveillance avancée et l'atténuation des cybermenaces pour les services du Canada à l'échelle de l'hôte géré par le gouvernement et de la couche réseau, pour les composants gérés par le Canada seulement.

7.20.24 Avis

- (1) L'entrepreneur doit fournir :

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

7.20.25 Gestion des incidents de sécurité

- (1) Le processus d'intervention en cas d'incident de sécurité d'entrepreneur pour les services doit englober les pratiques du cycle de vie de la gestion des incidents de sécurité informatique et les pratiques d'appui des activités de préparation, de détection, d'analyse, de confinement et de récupération, conformément à l'une des normes suivantes : i) ISO/IEC 27035:2011 Technologies de l'information -- Techniques de sécurité -- Management des incidents liés à la sécurité de l'information; ou ii) NIST SP800-612, Computer Security Incident Handling Guide; ou iii) Plan de gestion des événements de cybersécurité du gouvernement du Canada (PGECC GC) (<https://www.canada.ca/fr/secretaire-at-conseil-tresor/services/acces-information-protection-reseignements-personnels/gestion-securite-identite/plan-gestion-evenements-cybersecurite-gouvernement-canada.html>); ou (iv) autres pratiques exemplaires des principaux entrepreneurs de services si le Canada détermine, à sa discrétion, que celles-ci respectent ses exigences en matière de sécurité.
- (2) Le processus d'intervention en cas d'incident de sécurité d'entrepreneur doit comprendre ce qui suit :
- (a) des processus et procédures documentés indiquant comment l'entrepreneur relèvera les incidents de sécurité, y donnera suite et y remédiera, dressera un rapport à leur sujet et les signalera au Canada, y compris : (i) la portée des incidents de sécurité que l'entrepreneur doit signaler au Canada; (ii) le degré de divulgation et les mesures utilisées par l'entrepreneur pour détecter les incidents de sécurité, ainsi que les interventions connexes d'entrepreneur pour des types précis d'incidents de sécurité; (iii) le délai cible de signalement et de transmission des incidents de sécurité; (iv) la procédure de signalement et d'acheminement en cas

d'incidents de sécurité; (v) les coordonnées des personnes-ressources pour le traitement des enjeux relatifs aux incidents de sécurité; (vi) tout recours applicable à certains incidents de sécurité.

- (b) des procédures pour répondre aux demandes de preuve numérique potentielle ou d'autres renseignements provenant de l'environnement de service ou de l'infrastructure d'entrepreneur, y compris les procédures judiciaires et les mesures de protection pour la tenue d'une chaîne de possession des actifs d'information stockés ou traités par l'entrepreneur ou un sous-traitant d'entrepreneur. Les pratiques et les contrôles en matière d'éléments de preuve judiciaires et numériques doivent être conformes aux pratiques des principaux entrepreneurs de services, comme celles décrites dans la norme NIST 800-62 (Guide to Integrating Forensic Techniques into Incident Response), la norme ISO 27037 (Lignes directrices pour l'identification, la collecte, l'acquisition et la préservation de preuve numérique), ou une norme équivalente approuvée par écrit par le Canada.

7.20.26 Intervention en cas d'incident de sécurité

- (1) L'entrepreneur doit alerter et aviser promptement le Canada (par téléphone et par courriel) de toute compromission, de toute violation ou de toute preuve comme i) un incident de sécurité, ii) une défectuosité liée à la sécurité d'un actif, iii) l'accès irrégulier ou non autorisé à un actif, iv) la copie à grande échelle d'un actif d'information ou v) toute autre activité illégale recensée par l'entrepreneur, portant ce dernier à croire de manière raisonnable que le risque de compromission, d'atteinte à la sécurité ou à la vie privée est ou pourrait être imminent, ou si les mesures de protection existantes ont cessé de fonctionner, au cours de la période suivante (tous les jours, 24 heures par jour, 365 jours par année), et sans tarder, dans tous les cas, dans les 24 heures.
- (2) L'entrepreneur prend connaissance d'une violation de la sécurité entraînant la destruction, la perte, l'altération, la divulgation non autorisée des données ou l'accès accidentel ou illégal aux données du client ou des données personnelles du client pendant le traitement par l'entrepreneur (chacun étant un « incident de sécurité »), l'entrepreneur doit rapidement et sans tarder (i) informer le Canada de cet incident de sécurité; (ii) mener une enquête et fournir des renseignements détaillés sur cet incident de sécurité; (iii) prendre les mesures raisonnables pour atténuer les effets et les dommages découlant de l'incident de sécurité.
- (3) L'entrepreneur doit collaborer avec le Canada au confinement, à l'éradication et à la récupération des incidents de sécurité conformément au processus d'intervention en cas d'incident de sécurité d'entrepreneur et au Plan de gestion des événements de cybersécurité du gouvernement du Canada (PGECC GC) (<https://www.canada.ca/fr/secretariat-conseil-tresor/services/acces-information-protection-reseignements-personnels/gestion-securite-identite/plan-gestion-evenements-cybersecurite-gouvernement-canada.html>). En font partie :
 - (a) Ne permettre qu'aux représentants désignés du Canada :
 - a. de demander et de recevoir des renseignements liés à l'incident de sécurité et à tout actif d'information compromis (y compris, données des utilisateurs, journaux d'événements du système et de sécurité, saisies de paquets du réseau ou de l'hôte, journaux de composants de sécurité comme des systèmes de détection et de prévention d'intrusion et des pare-feu, etc.), dans un format non chiffré, à des fins de réalisation d'enquêtes;
 - b. d'assurer le suivi de l'état d'un événement signalé lié à la sécurité de l'information ou d'un incident de sécurité.
 - (b) d'appuyer les efforts d'enquête du Canada dans le cas de toute compromission des utilisateurs ou des données du service relevé.
- (4) L'entrepreneur doit :
 - (a) Tenir un registre des violations de la sécurité comprenant une description de la violation de la sécurité, la durée, les conséquences de la violation, le nom de la personne ayant signalé la violation, et la personne à qui la violation a été signalée, et la procédure pour récupérer les données ou le service;

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

7.20.27 Preuve électronique et mises en suspens pour raisons juridiques

L'entrepreneur doit (et doit, dans la mesure où cela s'applique compte tenu de la nature des services sous-traités fournis par chaque sous-traitant d'entrepreneur, exiger des sous-traitants qu'ils prennent des mesures raisonnables pour) s'assurer que les services offrent des fonctions de communication de la preuve électronique et de mises en suspens pour raisons juridiques pour les journaux des événements de sécurité afin de permettre au Canada de mener rapidement et efficacement des enquêtes de sécurité et de répondre aux demandes des tribunaux en matière de mises en suspens pour raisons juridiques.

7.20.28 Fuite d'information

- (1) L'entrepreneur doit fournir au Canada un document décrivant le processus qu'il suit pour répondre à un incident de fuite d'information. Le processus d'entrepreneur doit être harmonisé i) aux directives de la section IR-9 intitulée « Intervention en cas de fuite d'information » du document ITSG-33, ou ii) à une autre pratique exemplaire des principaux entrepreneurs de services approuvée par écrit par le Canada. Sans égard à ce qui précède, le processus d'intervention en cas de fuite d'information d'entrepreneur doit comprendre, à tout le moins :
 - (a) Un processus d'identification de l'actif d'information précis concerné par la contamination d'un actif ou d'un système;
 - (b) Un processus visant à isoler et à éradiquer un actif ou un système contaminé;
 - (c) Une description du processus d'identification des actifs ou systèmes qui ont pu avoir été subséquemment contaminés et de toute autre mesure prise pour empêcher la propagation de la contamination.
- (2) L'entrepreneur doit transmettre au Canada un processus d'intervention en cas de fuite d'information à jour, et ce, chaque année ou après toute modification apportée au processus de gestion de ces incidents.

7.20.29 Évaluation de la sécurité et preuve d'autorisation

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

7.20.30 Filtrage de sécurité du personnel

- (1) L'entrepreneur doit (et dans la mesure où cela s'applique compte tenu de la nature des services sous-traités rendus par chaque sous-traitant d'entrepreneur, doit exiger des sous-traitants qu'ils prennent des mesures raisonnables pour)
 - (a) Effectuer une vérification préalable de la diligence raisonnable de tout le personnel des services avant de recevoir l'autorisation d'accéder aux systèmes ou aux actifs d'information d'entrepreneur;
 - (b) Mettre en œuvre des mesures de sécurité qui accordent et maintiennent le degré requis de filtrage de sécurité pour le personnel des services, conformément à leurs privilèges d'accès aux systèmes dans lesquels les renseignements sont stockés et traités.
- (2) Les mesures de contrôle d'entrepreneur doivent être appliquées conformément à la définition et aux pratiques énoncées dans la Norme sur le filtrage de sécurité du Conseil du Trésor (<https://www.tbs-sct.gc.ca/pol/doc-fra.aspx?id=28115>), ou utiliser un équivalent acceptable convenu par le Canada. Cela comprend au minimum :
 - (a) Une description des postes des employés et des sous-traitants qui ont besoin d'un accès aux actifs d'information ou qui ont la capacité d'influencer la confidentialité, l'intégrité ou la disponibilité d'un actif d'information;
 - (b) Le 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 causent des doutes ou des préoccupations;

- (c) Le processus visant à s'assurer que les employés et les sous-traitants connaissent, comprennent et respectent leurs responsabilités en matière de sécurité de l'information et que le rôle que l'on compte leur confier leur convient;
- (d) Le processus qui est appliqué lorsqu'un employé ou un sous-traitant change de rôle ou au moment d'une cessation d'emploi;
- (e) Le processus relatif à la sensibilisation et à la formation en matière de sécurité données à l'arrivée des employés et lorsque les rôles des employés et sous-traitants changent;
- (f) L'approche de détection des initiés malveillants potentiels et les contrôles mis en œuvre pour atténuer le risque d'accès aux données du GC ou de dommage à la fiabilité des services d'infonuagique hébergeant les actifs et données du GC.

7.20.31 Installations des centres de données

- (1) L'entrepreneur doit mettre en place des mesures de sécurité qui assurent la protection des installations de TI et des actifs du système d'information dans lesquels les actifs et les actifs d'information sont stockés et protégés contre toute forme de manipulation, de perte, de dommages et de saisie. Des mesures de protection physique visant toutes les installations qui abritent des données et des actifs d'information du Canada doivent être appliquées conformément à une approche fondée sur les risques reposant sur la prévention, la détection, l'intervention et la récupération en matière de sécurité physique ou utiliser une telle approche, conformément aux mesures de contrôle et aux pratiques en matière de sécurité physique figurant dans les lignes directrices et les normes de la Gendarmerie royale du Canada (GRC) sur la sécurité physique. Les mesures de sécurité exigées en vertu de cette disposition comprennent, à tout le moins :

- (a) Des capacités suffisantes de redondance et de reprise dans les installations d'entrepreneur et entre celles-ci, qui sont notamment suffisamment disparates sur le plan géographique pour que la perte d'une installation n'empêche pas la récupération des données et des actifs d'information conformément aux engagements de niveau de service prescrits;
- (b) L'utilisation adéquate des supports de TI;
- (c) La maintenance contrôlée de tous les actifs et systèmes d'information et de leurs composants pour protéger leur intégrité et assurer leur disponibilité continue;
- (d) L'accès contrôlé aux dispositifs de sortie des systèmes d'information pour empêcher l'accès non autorisé aux données et aux actifs d'information du gouvernement du Canada;
- (e) Le contrôle et la gestion des dispositifs d'accès physique;
- (f) La restriction de l'accès physique aux actifs et aux emplacements de service au personnel de service autorisé en fonction du poste ou du rôle et du principe du besoin d'accès, validé par deux formes d'identification;
- (g) L'escorte des visiteurs et la surveillance de leurs activités;
- (h) L'application de mesures de protection des données du gouvernement du Canada à d'autres lieux de travail (p. ex. les sites de télétravail);
- (i) La consignation et la surveillance de tous les accès physiques aux emplacements de service et de tous les accès par voie électronique aux systèmes qui hébergent les données et les systèmes d'information, au moyen d'une combinaison de registres d'accès et de mécanismes de surveillance et de détection des intrusions.

7.20.32 Gestion de la chaîne d'approvisionnement

- (1) L'entrepreneur des services doit prendre des mesures de sécurité pour atténuer les menaces et les vulnérabilités associées à la chaîne d'approvisionnement des services de TI en vue de préserver la confiance en ce qui concerne la sécurité des sources des systèmes d'information et les composants de TI servant à offrir les services. En font notamment partie la conception et la mise en œuvre de contrôles

visant à atténuer et à contenir les risques liés à la sécurité des données par une séparation adéquate des tâches, un accès établi selon les fonctions des utilisateurs et un accès qui suit le principe du privilège minimal pour tout le personnel au sein de la chaîne d'approvisionnement.

- (2) L'entrepreneur doit présenter au Canada un « plan de gestion des risques de la chaîne d'approvisionnement (GRCA) » qui décrit l'approche d'entrepreneur en matière de GRCA et montre en quoi l'approche d'entrepreneur en matière de GRCA réduira et atténuera ces risques. Le plan de gestion des risques de la chaîne d'approvisionnement doit être conforme à l'une des pratiques exemplaires suivantes et être évalué et validé par un tiers indépendant certifié en vertu de l'American Institute of Certified Public Accountants (AICPA) ou de CPA Canada (Comptables professionnels agréés du Canada), ou encore du régime de certification ISO : i) ISO/IEC 27036 Technologies de l'information – Techniques de sécurité – Sécurité d'information pour la relation avec l'entrepreneur (parties 1 à 4); ii) NIST Special Publication 800-161 – Supply Chain Risk Management Practices for Federal Information Systems and Organizations; ou iii) catalogue des contrôles de sécurité ITSG-33, section SA-12, où les mesures de sécurité établies et structurées sont décrites dans un plan de gestion des risques de la chaîne d'approvisionnement (GRCA).

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

- (a) Présenter une mise à jour confirmant que l'approche et le plan de GRCA a été évaluée et validée par un tiers indépendant certifié selon les exigences de l'AICPA, de CPA Canada ou du régime de certification ISO.

OU

- (b) Présenter au Canada un prototypage du plan de GRCA, annuellement ou sur demande du Canada.

- (4) Dans le cas où l'entrepreneur est un éditeur de logiciel-service utilisant un entrepreneur d'aaS approuvé par le GC qui se conforme déjà aux exigences de l'article 13 – Gestion des risques de la chaîne d'approvisionnement, l'éditeur de logiciel-service utilisant un entrepreneur d'aaS approuvé par le GC doit fournir dans les 90 jours suivant l'attribution du contrat une liste de produits TIC qui décrit l'équipement TIC déployé dans un environnement d'aaS approuvé par le GC pour un examen de l'intégrité de la chaîne d'approvisionnement (ICA). Cet examen de l'ICA sera effectué au plus tôt tous les trois ans.

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

- (1) Les parties reconnaissent que, dans le cadre du présent contrat, le Canada considère la sécurité comme un facteur crucial et qu'une évaluation continue du logiciel-service sera nécessaire tout au long de la période visée par le contrat.
- (2) Les parties reconnaissent que le Canada se réserve le droit d'examiner le logiciel-service natif de tout entrepreneur, en tout ou en partie, en tout temps, pour des raisons d'intégrité de la chaîne d'approvisionnement. Cette reconnaissance n'oblige pas l'entrepreneur à appuyer l'examen de l'ICA.

- (3) Tout au long de la période du contrat, l'entrepreneur doit transmettre au Canada des renseignements relatifs à toute violation des données sur son réseau dont il a connaissance, qui entraîne a) un accès illégal au contenu canadien stocké sur l'équipement ou les installations d'entrepreneur, ou b) un accès non autorisé à cet équipement ou à ces installations, lorsque cet accès entraîne la perte, la divulgation ou la modification du contenu du Canada relativement à un changement de propriété, au logiciel-service en vertu du présent contrat, qui pourrait compromettre l'intégrité, la confidentialité, la disponibilité ou la cohérence, les mesures de vérification et les contrôles de l'accès du système ou des données et des applications du Canada.

7.20.34 Changement de contrôle

- (1) Si le Canada détermine, à sa seule discrétion, qu'un changement de contrôle dans l'entreprise d'entrepreneur (concernant aussi bien l'entrepreneur lui-même que l'une de ses sociétés mères, jusqu'au premier propriétaire) peut porter atteinte à la sécurité nationale, le Canada

peut résilier le contrat sans fautes en avisant l'entrepreneur dans les 90 jours suivant l'avis de changement de contrôle d'entrepreneur. Le Canada ne devra pas justifier la résiliation de contrat en raison d'un changement de contrôle si le Canada détermine, à sa discrétion, que ces justifications elles-mêmes pourraient porter atteinte à la sécurité nationale.

(2) Si le Canada détermine, à sa discrétion, qu'un changement de contrôle touchant un sous-traitant (concernant aussi bien le sous-traitant lui-même que l'une de ses sociétés mères, jusqu'au premier propriétaire) pourrait porter atteinte à la sécurité nationale, le Canada informera l'entrepreneur par écrit de sa décision. Le Canada ne sera pas tenu de justifier sa décision s'il détermine, à sa discrétion, que ces justifications elles-mêmes pourraient porter atteinte à la sécurité nationale. L'entrepreneur devra, dans les 30 jours civils suivant la réception de l'avis, prendre des arrangements avec un autre sous-traitant, que le Canada juge acceptable, pour la prestation de la partie des services d'infonuagique menés par le sous-traitant actuel (ou l'entrepreneur devra effectuer lui-même cette partie des services d'infonuagique). Si l'entrepreneur ne le fait pas dans le délai prescrit, le Canada pourra résilier le contrat sans faute en fournissant un avis à l'entrepreneur dans les 120 jours civils suivant la réception du premier avis de changement de contrôle d'entrepreneur.

(3) Dans cet article, une résiliation sans fautes signifie qu'aucune des parties n'est tenue responsable en ce qui a trait au changement de contrôle et à la subséquente résiliation, et le Canada ne devra payer que pour les services ayant été fournis avant la date d'entrée en vigueur de la résiliation.

(4) Malgré ce qui précède, le droit à la résiliation sans fautes du Canada ne s'applique pas dans les circonstances où une réorganisation interne n'affecte pas la propriété de la société mère (personne morale ou société de personnes) d'entrepreneur ou du sous-traitant, selon le cas, c'est à dire, le Canada n'a pas le droit de résilier un CONTRAT en vertu de cet article si l'entrepreneur ou le sous-traitant est contrôlé, en tout temps, directement ou indirectement, par le même propriétaire final.

7.20.35 Sous-traitants

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

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

7.20.36 Gestion des comptes principaux et racines

(1) L'entrepreneur doit protéger de manière adéquate le processus de gestion des comptes et de gestion de la facturation utilisé par le Canada et les services fournis au Canada, y compris les services fournis ou habilités par l'intermédiaire d'un revendeur de services d'infonuagique. Les mesures de sécurité comprennent notamment, sans s'y limiter :

- (a) limiter l'accès aux seuls utilisateurs qui sont autorisés à exécuter des transactions et des fonctions comme la création et l'émission de comptes maîtres et la facturation;
- (b) garantir la séparation des fonctions des personnes;
- (c) utiliser le principe de privilège minimal, y compris en ce qui concerne les fonctions spécifiques de sécurité et les comptes privilégiés;

- (d) s'assurer que les utilisateurs autorisés sont sensibilisés à la sécurité et suivent une formation en matière de sécurité dans le cadre de l'intégration à l'emploi et en cas de changement de rôle, et qu'ils sont au courant des exigences relatives à la sécurité associées au contrat.
- (e) créer, protéger et conserver les dossiers de vérification liés aux activités à l'appui de la gestion des comptes des services fournis au Canada;
- (f) fournir au Canada des rapports sur les événements vérifiés liés aux mesures relatives à l'émission et à la gestion des comptes principaux utilisés par le personnel pour gérer les comptes du gouvernement du Canada;
- (g) mettre en œuvre des mesures de sécurité qui accordent et maintiennent le degré requis de filtrage de sécurité pour le personnel à l'appui de la gestion des comptes principaux liés au Canada, conformément aux exigences de la Liste de vérification des exigences relatives à la sécurité (LVERS) et à celles relatives aux informations en nuage « Protégé B », et
- (h) assurer que les biens et les biens d'information sont protégés pendant les actions du personnel telles que les cessations d'emploi et les mutations, et après celles-ci.
- (i) assurer que les justificatifs d'identité demeurent à l'intérieur des frontières géographiques du Canada.

7.21 Obligations en matière de confidentialité

7.21.1 Objet

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

7.21.2 Transfert des obligations en matière de confidentialité

Les obligations d'entrepreneur contenues dans les présentes obligations en matière de confidentialité doivent être transférées par l'entrepreneur à ses sous-traitants, dans la mesure où elles s'appliquent à chaque sous-traitant d'entrepreneur, étant donné la nature des services fournis par celui-ci à l'entrepreneur.

7.21.3 Gestion des modifications

- (1) Tout au long du contrat, l'entrepreneur doit prendre toutes les mesures nécessaires, par l'intermédiaire des procédures de gestion des modifications, pour mettre à jour et maintenir les exigences en matière de confidentialité afin de se conformer aux pratiques en matière de confidentialité des normes de l'industrie, dans la mesure où si ces modifications peuvent raisonnablement être apportées sans ressources supplémentaires, l'entrepreneur doit les effectuer sans frais supplémentaires pour le Canada (c'est-à-dire par une autorisation de modification sans coût).
- (2) L'entrepreneur doit informer le Canada de toutes les améliorations qui pourraient avoir une incidence sur les services dans le contrat, y compris les améliorations techniques, administratives ou d'autres types d'améliorations. L'entrepreneur accepte d'offrir toutes les améliorations qu'il offre à ses clients en général dans le cadre de son offre de service standard, sans supplément pour le Canada.

7.21.4 Reconnaissance

- (1) Les parties reconnaissent que :
 - (a) Tous les biens et biens d'information sont assujettis à ces obligations en matière de confidentialité.

(b) Nonobstant toute autre disposition de la présente annexe, les parties partagent la responsabilité de l'élaboration et du maintien des politiques, des procédures et des contrôles de confidentialité relatifs aux biens et aux biens d'information.

(c) L'entrepreneur ne doit pas avoir ou tenter d'obtenir la garde d'un bien d'information, ni permettre au personnel des services d'accéder à un bien d'information avant la mise en œuvre des exigences en matière de confidentialité, comme l'exige la présente annexe, au plus tard à la date de mise en service ou avant.

7.21.5 Protection des biens d'information

Les données du Canada, notamment tous les renseignements personnels (RP), ne seront utilisées ou autrement traitées que pour fournir au Canada les services, y compris à des fins compatibles avec la prestation de ces services. L'entrepreneur ne doit pas utiliser ou autrement traiter les données du Canada ni en tirer de l'information à des fins publicitaires ou commerciales similaires. Entre les parties, le Canada conserve tous les droits, titres et intérêts relatifs aux données clients. L'entrepreneur n'acquiert aucun droit sur les données du client, à l'exception des droits que le client accorde à l'entrepreneur pour fournir les services au client.

7.21.6 Assurance d'une tierce partie : Certifications

(1) L'entrepreneur doit s'assurer que tous les renseignements personnels qu'il peut héberger, stocker ou traiter sur tous les biens, l'infrastructure d'entrepreneur (y compris tout service laas, PaaS ou ANS fourni au Canada) et les emplacements de service sont conformes aux certifications industrielles suivantes :

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

(2) L'entrepreneur doit démontrer sa conformité à cette certification en fournissant des rapports d'évaluation ou des attestations de tiers indépendants pour toutes les parties du service.

(3) Chaque certification fournie doit : (i) déterminer la raison sociale légale d'entrepreneur ou du sous-traitant d'entrepreneur concerné; (ii) déterminer la date de certification d'entrepreneur ou du sous-traitant d'entrepreneur, notamment la date de certification d'entrepreneur de services d'infonuagique et le statut de cette certification; (iii) déterminer la liste des biens, des infrastructures d'entrepreneur et des emplacements du service dans le cadre du rapport de certification. Si la méthode créée est utilisée pour exclure les organisations de sous-services comme la prise en charge de centres de données, le rapport d'évaluation de l'organisation de sous-services doit être joint.

(4) Chaque certification ISO fournie en vertu de la présente section doit être valide pendant toute la durée du contrat, dans les 12 mois précédant le début du contrat. Les certifications doivent être accompagnées de rapports d'évaluation ISO à l'appui.

(5) L'entrepreneur doit maintenir la validité de sa certification selon les normes décrites au paragraphe 5(1) pendant toute la durée du contrat. L'entrepreneur doit fournir, au moins une fois par année, et sans délai à la demande du Canada, tous les rapports ou dossiers qui peuvent être raisonnablement requis pour démontrer que les certifications d'entrepreneur demeurent à jour et sont valides pour la durée du contrat.

7.21.7 Conformité aux exigences en matière de confidentialité

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

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

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

(2) Cela s'applique à toutes les informations, données et métadonnées détenues ou gardées par l'entrepreneur ou qui sont acquises en vertu des responsabilités et obligations d'entrepreneur en vertu du présent contrat ou qui sont liées de quelque autre façon à ces responsabilités et à ces obligations. L'entrepreneur reconnaît que cela est nécessaire afin d'assurer que le Canada peut se fonder sur les renseignements, données et métadonnées en vue de s'acquitter de ses propres obligations juridiques, notamment celles imposées par la loi. Cela permet également de garantir que les informations, données et métadonnées peuvent être utilisées comme preuve convaincante devant un tribunal.

7.21.8 Audit de conformité

(1) Dans le cas où le Canada doit effectuer des audits de sécurité, des inspections ou examiner d'autres renseignements (documentation, description de protection de données, architecture de données et descriptions de sécurité), les deux parties conviennent de négocier de bonne foi pour trouver une solution et de tenir compte à la fois de la justification de la demande du Canada et des processus et protocoles d'entrepreneur.

(2) Dans les 30 jours suivant l'attribution du contrat, l'entrepreneur doit retenir les services d'une tierce partie pour effectuer un audit de la confidentialité ou fournir la preuve qu'il ne produit, ne recueille, n'utilise, ne stocke ni ne communique aucun renseignement personnel supplémentaire tel que défini par le Canada, autre que les données du client telles que définies par l'entrepreneur, et ne possède pas spécifiquement de PII dans les données de soutien (recueillies dans des journaux [par exemple, les données téléométriques telles que les en-têtes et le contenu d'un message électronique]).

(3) L'entrepreneur doit effectuer les audits de confidentialité et de sécurité de la sécurité des ordinateurs, de l'environnement informatique et des centres de données physiques qu'il utilise pour traiter les données du Canada de la façon suivante :

- (a) Lorsqu'une norme ou un cadre prévoit des vérifications, une vérification de cette norme ou de ce cadre de contrôle sera entreprise au moins une fois par année;
- (b) Chaque audit sera effectué conformément aux normes et règles de l'organisme de réglementation ou d'accréditation pour chaque norme ou cadre de contrôle applicable;
- (c) Chaque audit sera effectué par des auditeurs de sécurité tiers qualifiés, indépendants et qui (i) sont qualifiés selon l'American Institute of Certified Public Accountants (AICPA) ou CPA Canada (Comptables professionnels agréés du Canada) ou selon le régime de certification ISO, et (ii) respectent la norme ISO/CEI 17020 sur les systèmes de gestion de la qualité au choix et aux frais d'entrepreneur.

(4) Chaque audit donnera lieu à la production d'un rapport d'audit qui doit être communiqué au Canada. Le rapport d'audit doit indiquer clairement toutes les constatations importantes faites par l'auditeur. L'entrepreneur doit corriger rapidement et à la satisfaction de l'auditeur les problèmes soulevés dans tout rapport d'audit et doit (i) fournir au Canada le plan pour corriger toute constatation négative découlant de ces rapports et (ii) fournir au Canada, sur demande, des rapports d'étape sur la mise en œuvre dans un délai de dix jours ouvrables du gouvernement fédéral.

(5) À la demande du Canada, l'entrepreneur ou un sous-traitant peut fournir des renseignements supplémentaires sur l'entrepreneur, y compris des plans de sécurité, des conceptions ou des documents d'architecture du système qui offrent une description complète du système, afin

de compléter les rapports de certification et d'audit décrits dans la présente et de démontrer la conformité d'entrepreneur avec les certifications requises de l'industrie.

7.21.9 Demandes de propriété des données et de confidentialité

(1) Les données du client, y compris toutes les informations personnelles (IP), ne seront utilisées ou traitées que pour fournir au client les services d'infonuagique, y compris à des fins compatibles avec la fourniture de ces services. L'entrepreneur ne doit pas utiliser ou autrement traiter les données du client ni en tirer de l'information à des fins publicitaires ou commerciales similaires. Entre les parties, le client conserve tous les droits, titres et intérêts relatifs aux données du client. L'entrepreneur n'acquiert aucun droit sur les données du client, à l'exception des droits que le client accorde à l'entrepreneur pour fournir les services d'infonuagique au client.

(2) Toutes les données qu'il stocke, héberge ou traite au nom du Canada demeurent la propriété du Canada. À la demande de l'autorité contractante, l'entrepreneur doit fournir les dossiers des informations personnelles dans les deux jours ouvrables du gouvernement fédéral (ou cinq jours ouvrables du gouvernement fédéral, s'ils doivent être récupérés à partir d'une sauvegarde/réplication hors site) dans un document Word ou Excel.

7.21.10 Agent de protection de la vie privée

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

7.21.11 Aider à la réalisation de l'évaluation des facteurs relatifs à la vie privée du Canada

L'entrepreneur doit aider le Canada à réaliser une évaluation des facteurs relatifs à la vie privée conformément à la directive du Conseil du Trésor sur l'évaluation des facteurs relatifs à la vie privée, en aidant le Canada à produire les documents justificatifs, notamment une évaluation des facteurs relatifs à la vie privée de base pour le Canada fournie par l'entrepreneur. L'entrepreneur s'engage à fournir ce soutien dans les cinq à dix jours ouvrables suivant une demande ou dans un délai convenu d'un commun accord, selon la complexité de la demande du Canada.

7.21.12 Atteinte à la vie privée

(1) L'entrepreneur doit aviser rapidement le responsable technique (par téléphone et par courriel) de toute compromission ou toute violation ou de tout fait qui amène l'entrepreneur de services d'infonuagique à croire qu'un risque de compromission ou de violation est ou peut être imminent, ou si des mesures de sécurité existantes ont cessé de fonctionner, et ce, au cours de la période suivante (7 jours sur 7, 24 heures sur 24, 365 jours sur 365), et dans le cadre des engagements de niveau de service d'entrepreneur de services d'infonuagique.

(2) Si l'entrepreneur prend connaissance d'une violation de la sécurité entraînant la destruction, la perte, l'altération, la divulgation non autorisée de données du client ou de données personnelles ou l'accès accidentel ou illégal à celles-ci pendant le traitement par l'entrepreneur (chaque événement étant considéré comme un « incident de sécurité »), l'entrepreneur doit rapidement et sans retard indu :

- a. aviser le Canada de l'incident de sécurité;

- b. enquêter sur l'incident de sécurité et fournir au Canada des renseignements détaillés sur cet incident, et
- c. prendre des mesures raisonnables pour atténuer les effets de l'incident de sécurité et limiter les dommages qui en découlent.

(3) L'entrepreneur doit :

- a. tenir un registre des atteintes à la sécurité avec une description de l'atteinte à la sécurité, la période de temps, les conséquences de l'atteinte, le nom du déclarant, la personne à qui l'atteinte a été signalée et la procédure de récupération des données, et
- b. assurer le suivi, ou permettre au Canada d'assurer le suivi des divulgations de données du Canada, y compris les données qui ont été divulguées, à qui, et à quel moment.

7.21.13 Propriété des renseignements personnels et des dossiers

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

7.21.14 Utilisation des renseignements personnels

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

7.21.15 Collecte de renseignements personnels

(1) Si l'entrepreneur/sous-traitant étranger destinataire doit recueillir des renseignements personnels auprès d'un tiers dans le cadre des travaux, il ne doit recueillir que les renseignements personnels nécessaires à l'exécution des travaux. L'entrepreneur/sous-traitant étranger destinataire doit recueillir les renseignements personnels auprès de la personne concernée et l'informer (au moment de la collecte ou préalablement) de ce qui suit :

- (a) les renseignements personnels sont recueillis au nom du Canada et lui seront transmis;
- (b) les usages qui seront faits des renseignements personnels recueillis;
- (c) que la divulgation des renseignements personnels est volontaire ou, s'il existe une obligation juridique de divulguer les renseignements personnels, les fondements de cette obligation juridique;
- (d) les conséquences, s'il en est, du refus de fournir les renseignements;
- (e) que l'intéressé a le droit d'accéder à ses renseignements personnels et d'y apporter des corrections;
- (f) que les renseignements personnels feront partie d'un fichier de renseignements personnels particulier (au sens de la *Loi sur la protection des renseignements personnels*), et également fournir à la personne de l'information concernant l'institution fédérale qui gère le fichier de renseignements personnels, si l'autorité contractante a fourni ces renseignements à l'entrepreneur/sous-traitant étranger destinataire.

(2) L'entrepreneur et le sous-traitant étrangers destinataires et leurs employés respectifs doivent s'identifier auprès des personnes desquelles ils recueillent des renseignements personnels et leur donner le moyen de vérifier qu'ils sont autorisés à recueillir les renseignements personnels conformément à un contrat conclu avec le Canada.

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

(4) Si, au moment de la collecte de renseignements personnels auprès d'une personne, l'entrepreneur/sous-traitant étranger destinataire soupçonne que cette personne n'est pas en mesure de consentir à la divulgation et à l'utilisation de ses renseignements personnels, l'entrepreneur/sous-traitant étranger destinataire doit demander des directives à l'autorité contractante.

7.21.16 Assurer l'exactitude, la confidentialité et l'intégrité des renseignements personnels

(1) L'entrepreneur/sous-traitant étranger destinataire doit veiller à ce que les renseignements personnels soient les plus exacts, complets et à jour que possible. L'entrepreneur/sous-traitant étranger destinataire doit veiller à protéger la confidentialité des renseignements personnels. À cette fin, l'entrepreneur/sous-traitant étranger destinataire doit, au minimum :

- (a) ne pas utiliser de données d'identification personnelle (p. ex. le numéro d'assurance sociale) pour lier plusieurs bases de données qui comprennent des renseignements personnels;
- (b) isoler tous les dossiers des renseignements et des dossiers d'entrepreneur/sous-traitant étranger destinataire;
- (c) ne donner l'accès aux renseignements personnels et aux dossiers qu'à ceux qui le requièrent aux fins d'exécution des travaux (par exemple, en utilisant des mots de passe ou un accès biométrique);
- (d) donner de la formation à toute personne à laquelle l'entrepreneur/sous-traitant étranger destinataire donne accès aux renseignements personnels concernant l'obligation d'assurer la confidentialité et de ne l'utiliser qu'aux fins d'exécution des travaux. L'entrepreneur/sous-traitant étranger destinataire doit donner cette formation avant d'autoriser l'accès aux renseignements personnels et préparer à cet effet un dossier accessible à l'autorité contractante, sur demande;
- (e) à la demande de l'autorité contractante, avant de donner accès à quiconque aux renseignements personnels, demander aux personnes auxquelles l'entrepreneur/sous-traitant étranger destinataire donne accès aux renseignements personnels de reconnaître, par écrit (sous une forme approuvée par l'autorité contractante), leurs responsabilités en matière de confidentialité des renseignements personnels;
- (f) tenir un registre de toutes les demandes faites par une personne pour la révision de ses renseignements personnels et de toutes les demandes de correction d'erreurs ou d'omissions concernant les renseignements personnels (que les demandes soient faites directement par une personne ou par le Canada au nom d'une personne);
- (g) joindre une note à tout dossier qu'une personne a demandé de corriger, mais que l'entrepreneur/sous-traitant étranger destinataire a décidé, pour quelque raison que ce soit, de ne pas corriger. Lorsque cela se produit, l'entrepreneur/sous-traitant étranger destinataire doit immédiatement informer l'autorité contractante de la correction demandée et des raisons pour lesquelles l'entrepreneur/sous-traitant étranger destinataire a décidé de ne pas l'effectuer. Si l'autorité contractante demande que la correction soit effectuée, l'entrepreneur a l'obligation de le faire;
- (h) consigner la date et l'auteur de la dernière mise à jour de chaque dossier;
- (i) maintenir un journal de vérification électronique qui enregistre tous les accès et les tentatives d'accès aux dossiers électroniques. Le journal de vérification doit être dans un format qui peut être lu par l'entrepreneur/sous-traitant étranger destinataire et le Canada en tout temps, et

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

7.21.17 Protection des renseignements personnels

- (1) L'entrepreneur/sous-traitant étranger destinataire doit, en tout temps, protéger les renseignements personnels en prenant toutes les mesures raisonnablement nécessaires pour les protéger et en protéger l'intégrité et la confidentialité. À cette fin, l'entrepreneur/sous-traitant étranger destinataire doit, au minimum :
 - (a) stocker les renseignements personnels sous format électronique de manière à ce qu'un mot de passe (ou un mécanisme de contrôle similaire, comme l'accès biométrique) soit requis pour accéder au système ou à la base de données contenant les renseignements personnels;
 - (b) s'assurer que les mots de passe ou autres moyens d'accès aux renseignements personnels ne sont fournis qu'aux personnes qui le requièrent aux fins d'exécution des travaux;
 - (c) ne pas confier à un tiers (y compris une société affiliée) le stockage électronique des renseignements personnels sans l'autorisation préalable et écrite de l'ADS canadienne;
 - (d) protéger les bases de données ou les systèmes informatiques qui contiennent les renseignements personnels contre un accès externe au moyen de méthodes couramment utilisées de temps à autre par des organismes publics et privés du Canada faisant preuve de prudence dans le but de protéger les renseignements très protégés et hautement sensibles;
 - (e) faire une sauvegarde sécurisée et une mise à jour de tous les dossiers au moins une fois par semaine;
 - (f) mettre en œuvre toutes les mesures de sécurité ou de protection raisonnables demandées par le Canada de temps à autre;
 - (g) aviser immédiatement l'autorité contractante et l'ADS canadienne de toute atteinte à la sécurité; par exemple, chaque fois qu'une personne non autorisée obtient l'accès aux renseignements personnels.

7.21.18 Obligations réglementaires

- (1) L'entrepreneur/sous-traitant étranger destinataire reconnaît que le Canada est tenu de traiter les renseignements personnels et les dossiers conformément aux dispositions de la *Loi sur la protection des renseignements personnels*, de la *Loi sur l'accès à l'information*, L.R.C. 1985, ch. A-1, et de la *Loi sur la Bibliothèque et les Archives du Canada*, L. C. 2004, ch. 11. L'entrepreneur/sous-traitant étranger destinataire convient de se conformer aux exigences établies par l'autorité contractante qui sont raisonnablement requises pour permettre au Canada de remplir ses obligations en vertu de ces lois et de toute autre loi qui entre en vigueur lorsqu'il y a lieu.
- (2) L'entrepreneur/sous-traitant étranger destinataire reconnaît que les obligations dont il doit s'acquitter en vertu du contrat ou du contrat de sous-traitance s'ajoutent à toutes celles qui lui incombent en vertu de la *Loi sur la protection des renseignements personnels* et les *documents électroniques*, L.C. 2000, ch. 5, ou d'une loi similaire en vigueur dans une province ou un territoire du Canada. Si l'entrepreneur/sous-traitant étranger destinataire croit que l'une des obligations du contrat ou du contrat de sous-traitance l'empêche de s'acquitter de ses obligations en vertu de ces lois, il doit immédiatement aviser l'autorité contractante de la disposition particulière du contrat ou du contrat de sous-traitance et de l'obligation particulière de la loi qu'il considère comme contradictoires.

7.21.19 Obligation juridique de divulguer les renseignements personnels

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

7.21.20 Plaintes

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

7.21.21 Exception

Les obligations énoncées dans ces conditions générales supplémentaires ne s'appliquent pas aux renseignements personnels qui sont déjà du domaine public, du moment qu'ils ne sont pas devenus du domaine public, à la suite d'une faute ou d'une omission d'entrepreneur ou de l'un de ses sous-traitants, agents ou représentants, ou de l'un de leurs employés.

7.22 Programme de contrats fédéraux pour l'équité en matière d'emploi - Manquement de la part d'entrepreneur

L'entrepreneur comprend et convient que, lorsqu'il existe une entente pour la mise en œuvre de l'équité en matière d'emploi entre lui-même et Emploi et Développement social Canada (EDSC) – Travail, cette entente doit demeurer en vigueur pendant toute la durée du contrat. Si l'entente n'est plus en vigueur, le nom d'entrepreneur sera ajouté à la Liste d'admissibilité limitée à soumissionner au Programme de contrats fédéraux (PCF). L'imposition d'une telle sanction par EDSC constituera un manquement de la part d'entrepreneur, selon les modalités du contrat.

7.23 Ordre de priorité des documents

- (1) En cas de contradiction entre le libellé des documents énumérés dans la liste, c'est le libellé du document qui figure en premier dans la liste qui l'emporte sur celui de tout autre document qui figure plus bas dans ladite liste.
- (a) les articles de la convention, notamment toutes les clauses du Guide des clauses et conditions uniformisées d'achat (CCUA) intégrées par renvoi dans ces articles de la convention;
 - (b) l'Annexe A – Énoncé des besoins;
 - (c) l'Annexe B – Base de paiement;
 - (d) l'Annexe C – Liste de vérification des exigences relatives à la sécurité (s'il y a lieu);
 - (e) l'Annexe D – Processus d'intégrité de la chaîne d'approvisionnement;
 - (f) les autorisations de tâches signées (y compris toutes leurs annexes, le cas échéant);
 - (g) la soumission d'entrepreneur en date du ____ (insérer la date de la soumission);
 - (h) L'Annexe « H » - Programme d'évaluation de la sécurité des TI logiciels-services : processus d'intégration
 - (i) l'accord sur les niveaux de service (ANS) du ANS d'entrepreneur;
 - (j) l'Annexe G – Entente de non-divulgaration.

7.24 Ressortissants étrangers (entrepreneur canadien)

Clause du guide des CCUA A2000C (2006-06-16) Ressortissants étrangers (entrepreneur canadien)

Remarque à l'intention des soumissionnaires : On intégrera la présente clause ou la clause suivante dans le contrat subséquent selon que le soumissionnaire retenu est un entrepreneur canadien ou un entrepreneur étranger.

7.25 Ressortissants étrangers (entrepreneur étranger)

Clause du guide des CCUA A2001C (_____) (*insérer la date*) Ressortissants étrangers (entrepreneur étranger)

APPENDICE A - DÉFINITIONS ET INTERPRÉTATIONS

Dans le présent contrat, à moins que le contexte ne l'indique autrement, les termes ci-après ont les acceptions suivantes :

« Biens » : Toutes les ressources en matière de technologies de l'information auxquelles l'entrepreneur a accès ou les ressources de cette nature qu'il utilise ou gère pour assurer la prestation et la livraison des services décrits dans la présente entente (y compris, non exclusivement, toutes les ressources technologiques se trouvant aux points de services d'entrepreneur, ou encore, dans un centre de données, un réseau, un dispositif de stockage, des serveurs, des plateformes de virtualisation, des systèmes d'exploitation, des logiciels et des applications d'entrepreneur ou d'un sous-traitant de celui-ci).

Par « taxes applicables », on entend la taxe sur les produits et services (TPS), la taxe de vente harmonisée (TVH) et toute taxe provinciale, payable par le Canada, selon la loi, comme la taxe de vente du Québec (TVQ) en date du 1^{er} avril 2013.

« Taux moyen » désigne la moyenne arithmétique simple du taux d'escompte en vigueur chaque jour, à 16 h, heure de l'Est, pour le mois civil immédiatement antérieur à la date de paiement.

Le « taux d'escompte » s'entend du taux d'intérêt établi de temps à autre par la Banque du Canada qui représente le taux minimal auquel elle consent des avances à court terme aux membres de l'Association canadienne des paiements.

« Canada », « Couronne », « Sa Majesté » ou « l'État » désignent Sa Majesté la Reine du chef du Canada, représentée par le ministre des Travaux publics et des Services gouvernementaux, et toute autre personne dûment autorisée à agir au nom de ce dernier ou, s'il y a lieu, un ministre compétent à qui le ministre des Travaux publics et des Services gouvernementaux a délégué ses pouvoirs, fonctions ou attributions et toute autre personne dûment autorisée à agir au nom de ce ministre.

« Données du Canada » : renseignements ou données, quels qu'en soient la forme et le format :

- A. divulgués par le personnel, les clients, les partenaires, les participants à des coentreprises, les concédants de licence, les entrepreneurs ou les entrepreneurs du Canada ou liés à ceux-ci;
- B. divulgués par les utilisateurs finaux des services ou liés à ceux-ci, ou
- C. collectés, utilisés ou traités par, ou stockés pour, les Services; qui sont directement ou indirectement :
 - i. divulgués à l'entrepreneur ou aux sous-traitants par ou au nom du Canada ou des utilisateurs finaux;
 - ii. auxquels l'entrepreneur ou ses sous-traitants peuvent avoir accès, de façon intentionnelle ou accidentelle;
 - iii. résidant sur tout bien, ou sur tout autre réseau, système ou matériel utilisé ou géré pour le Canada par l'entrepreneur pour les services et les services d'entrepreneur, y compris l'infrastructure d'entrepreneur; ou
 - iv. générés, développés, acquis ou autrement obtenus par l'entrepreneur, sous-traitant étranger ou sous-traitant ultérieur dans le cadre ou au cours de la fourniture des services; et comprennent tous les renseignements dérivés de ces renseignements et toutes les métadonnées liées ou intégrantes à ces renseignements. Il est entendu que les « données du Canada » comprennent la totalité de l'information et des données stockées ou traitées par l'entremise des services, des biens ou de l'infrastructure d'entrepreneur.

« Client » : le ministère ou l'organisme pour lequel on exécute les travaux ou les services dans le cadre du contrat. À ce titre, le terme « client » peut désigner un ministère, un établissement public, une agence ministérielle ou une autre entité de l'État décrits dans la *Loi sur la gestion des finances publiques* (avec ses modifications successives), et toute autre partie pour laquelle Travaux publics et Services gouvernementaux Canada a l'autorisation d'agir, le cas échéant, selon l'article 16 de la *Loi sur le ministère des Travaux publics et des Services gouvernementaux*.

« Données du client » : (i) toute donnée fournie à l'entrepreneur par le client, ou selon ses directives, en lien avec la solution et (ii) tout le contenu que l'entrepreneur développe et livre au client, et que ce dernier accepte, conformément au présent contrat.

L'« infonuagique » est un modèle qui permet, de façon omniprésente, pratique et à la demande, l'accès réseau à un bassin partagé de ressources informatiques configurables (p. ex. réseaux, serveurs, stockage, applications et services) qui peuvent rapidement être fournies et libérées avec un minimum d'effort de gestion et d'interaction avec l'entrepreneur.

« Infrastructure infonuagique » : un regroupement de logiciels et de matériel qui assurent les cinq caractéristiques essentielles de l'infonuagique. L'infrastructure infonuagique peut être considérée comme contenant à la fois une couche physique et une couche d'abstraction. La couche physique est formée des ressources logicielles nécessaires pour étayer les services infonuagiques fournis, et elle comporte normalement un serveur, du stockage et des composantes réseau. La couche d'abstraction comprend le logiciel déployé sur la couche physique, où prennent forme les caractéristiques infonuagiques essentielles. Conceptuellement, la couche d'abstraction se trouve au-dessus de la couche physique. [National Institute of Standards and Technology (NIST)]

« Entrepreneur de services infonuagiques » signifie l'entité qui possède, exploite et maintient l'infrastructure physique qui héberge une solution et à partir de laquelle cette dernière est distribuée. Un entrepreneur de services infonuagiques peut également être un éditeur de ANS s'il héberge et distribue des solutions qui lui appartiennent ou qui proviennent de tiers. « Disponible sur le marché » désigne un produit ou un service que le public peut utiliser ou consommer et qui n'exige aucune modification ni aucun entretien pendant son cycle de vie.

« Contrat » désigne les modalités du contrat, toutes les conditions générales, toutes les conditions générales supplémentaires, toutes les annexes, tous les appendices et tout autre document que l'un ou l'autre de ces documents incorpore par renvoi, compte tenu des modifications apportées avec l'accord des parties.

« Autorité contractante » : personne désignée comme telle dans le contrat, ou dans un avis à l'entrepreneur, pour représenter le Canada aux fins de l'administration du contrat.

« Entrepreneur » : l'entité désignée dans le contrat pour fournir les services et les travaux au Canada.

« Prix du contrat » : somme indiquée dans le contrat qui devra être payée à l'entrepreneur pour les travaux, excluant les taxes applicables.

« Coût » : le coût établi conformément aux Principes des coûts contractuels 1031-2 en vigueur à la date de la demande de soumissions ou, s'il n'y a pas eu de demande de soumissions, à la date du contrat.

« Date de paiement » : la date que porte le titre négociable tiré par le Receveur général du Canada afin de payer une somme exigible en vertu du contrat.

« Produits livrables » ou « livrables », termes qui, dans leur sens générique, renvoient à toute partie distincte du travail devant être effectué pour le Canada.

« Appareil » : équipement muni d'une unité centrale, d'une mémoire de grande capacité, d'unités d'entrée-sortie comme un clavier et un écran, et qui comprend les serveurs, les ordinateurs de bureau, les postes de travail, les ordinateurs portatifs, les assistants numériques personnels et l'équipement informatique mobile.

« Erreur » désigne toute instruction ou tout énoncé présent ou manquant dans la solution qui, par sa présence ou son absence, empêche la solution de fonctionner conformément aux spécifications.

« Jour ouvrable du gouvernement fédéral » : du lundi au vendredi, de 8 h à 16 h, heure normale de l'Est, à l'exception des jours fériés observés par le Canada.

« Infrastructure comme service », « infrastructure-service » ou « IaaS » : ces termes désignent la capacité permettant au consommateur d'obtenir des ressources de traitement, de stockage, de réseau, ainsi que d'autres ressources informatiques de base pour pouvoir ensuite déployer et exécuter les logiciels de son choix, y compris des systèmes d'exploitation et des applications. Le consommateur ne gère ni ne contrôle l'infrastructure

en nuage sous-jacente, mais il exerce un contrôle sur les systèmes d'exploitation, les unités de stockage et les applications déployées, et, dans certains cas et de façon limitée, sur certains éléments de réseau (comme les pare-feu hôtes).

« Infrastructure IaaS » : infrastructure gérée par l'entrepreneur et fournie comme service (p. ex. centre de données, réseautage, stockage, serveurs, plateforme de virtualisation). Cela comprend également les systèmes, le matériel et les logiciels servant à gérer, à exploiter et à fournir une infrastructure IaaS.

« Ressources d'information » : tout élément de données précis faisant partie des données du Canada.

« Fuite d'information » : incident au cours duquel une ressource d'information est placée accidentellement dans un bien ou un système n'ayant pas l'autorisation de la traiter (p. ex. ITSG-33, IR-9).

« PaaS », « plateforme comme service » ou « plateforme-service » : termes qui désignent la capacité qui permet au consommateur de déployer sur l'infrastructure infonuagique des applications qu'il a acquises ou créées à l'aide d'outils, de langages, de bibliothèques et de services de programmation pris en charge par l'entrepreneur. [NIST]

« Infrastructure PaaS » : infrastructure de la plateforme gérée par l'entrepreneur et fournie comme service (p. ex. centre de données, réseautage, stockage, serveurs, plateforme de virtualisation, système d'exploitation, intergiciel, Runtime). Cela comprend également les systèmes, le matériel et les logiciels servant à gérer, à exploiter et à offrir une infrastructure PaaS.

« Partie » signifie le Canada, l'entrepreneur ou tout autre signataire du contrat; « parties » signifie l'ensemble d'entre eux.

« Nuage public » désigne l'infrastructure infonuagique mise à la disposition du grand public. Il peut appartenir à une organisation commerciale, universitaire ou gouvernementale, ou à une combinaison de celles-ci, lesquelles en assurent la gestion et le fonctionnement. Il se trouve dans les locaux d'entrepreneur de services infonuagiques.

« Services publics et Approvisionnement Canada » ou « Travaux publics et Services gouvernementaux Canada » désigne le ministère des Travaux publics et des Services gouvernementaux, comme énoncé dans la *Loi sur le ministère des Travaux publics et des Services gouvernementaux*.

« En souffrance » désigne une somme qui demeure impayée le lendemain du jour où elle est devenue exigible en vertu du contrat.

« Renseignements personnels » : information qui a trait à une personne identifiable et qui est consignée dans tous les formats possibles, conformément à l'article 3 de la *Loi sur la protection des renseignements personnels*. Il s'agit, notamment, des renseignements relatifs à la race, à l'origine nationale ou ethnique, à la religion, à l'âge, à l'état matrimonial, à l'adresse, à l'éducation ainsi que des renseignements relatifs au dossier médical, au casier judiciaire, aux opérations financières et aux antécédents professionnels. Les renseignements personnels comprennent aussi tout numéro ou symbole qui est propre à une personne, comme son numéro d'assurance sociale. La définition est tirée du site Web de la législation (Justice) du gouvernement du Canada : <https://laws-lois.justice.gc.ca/fra/lois/P-21/section-3.html>

« Traiteur de l'information » : personne physique ou morale, autorité publique, organisme ou autre organisation qui effectue le traitement des renseignements personnels au nom du Canada, conformément aux directives de celui-ci.

« Fabricant du produit » : entité qui assemble les composantes en vue de la fabrication d'un produit.

« Nuage public » désigne l'infrastructure infonuagique mise à la disposition du grand public. Il peut appartenir à une organisation commerciale, universitaire ou gouvernementale, ou à une combinaison de celles-ci, lesquelles en assurent la gestion et le fonctionnement. Il se trouve dans les locaux d'entrepreneur de services infonuagiques.

« Services infonuagiques publics » : bassin partagé de modèles de services infonuagiques configurables rendus accessibles aux utilisateurs sur Internet en tant que service rapide, élastique, sur demande à partir des serveurs d'entrepreneur de services infonuagiques, par opposition aux serveurs qu'une compagnie possède sur place, mais qui ne comprennent pas les services gérés, les services infonuagiques privés, de formation

ou sur place, ou encore les services professionnels ou d'experts-conseils qui dépassent les services de soutien normaux offerts sur le marché au public.

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

Le « registre des incidents de sécurité » renvoie à tout incident, tout avis ou toute alerte qu'un dispositif, un système ou un logiciel peut techniquement produire en ce qui concerne son état, ses fonctions et ses activités. Les registres des incidents de sécurité ne se limitent pas aux dispositifs de sécurité; ils s'appliquent à tous les dispositifs, systèmes et logiciels ayant techniquement la capacité de produire des registres sur les incidents pouvant être utilisés dans les enquêtes sur la sécurité, les vérifications et les activités de surveillance. Voici une liste non exhaustive d'exemples de systèmes pouvant produire des registres des incidents de sécurité : pare-feu, systèmes de prévention d'intrusion, routeurs, commutateurs, filtrage de contenu, registres du flux de trafic d'un réseau, réseaux, services d'authentification, services de répertoire, protocoles DHCP, systèmes DNS, plateformes matérielles, plateformes de virtualisation, serveurs, systèmes d'exploitation, serveurs Web, bases de données, applications, pare-feu à couche application (couche 7).

« Incident de sécurité » : toute anomalie observable ou mesurable se rapportant à un bien et entraînant ou pouvant entraîner :

(A) une violation des politiques de sécurité du Canada, d'une mesure de sécurité en particulier, des politiques ou des procédures de sécurité d'entrepreneur ou d'un de ses sous-traitants, ou de toute exigence de ces obligations en matière de sécurité ou de protection de la vie privée; ou
(B) l'accès aux justificatifs d'un membre du personnel autorisé, aux justificatifs des utilisateurs finaux ou à des renseignements, ainsi que la modification ou l'exfiltration de ceux-ci, le tout sans autorisation.

« Accord sur les niveaux de service (ANS) » : une entente entre l'entrepreneur et le Canada qui définit le niveau de service attendu d'entrepreneur.

« Lieu de service » : toute installation ou tout site ou endroit que l'entrepreneur ou qu'un sous-traitant ultérieur d'entrepreneur possède, loue, fournit ou occupe autrement, et à partir duquel l'entrepreneur ou tout sous-traitant ultérieur d'entrepreneur fournit des services infonuagiques publics.

« Services » signifie :

- i) octroyer les droits d'utilisation des applications logicielles (« solutions »)
- ii) fournir la documentation de la solution;
- iii) maintenir, mettre à niveau et mettre à jour les solutions;
- iv) gérer les incidents et les défauts pour assurer le fonctionnement de la solution aux niveaux de service applicables;
- v) fournir les services d'infrastructure de technologie de l'information accessoires et supplémentaires qui sont nécessaires à la livraison de la solution.

« Logiciel comme service », « logiciel-service » ou « ANS » : un modèle de service qui permet au client d'utiliser les applications d'entrepreneur qui résident dans une infrastructure infonuagique. Les applications sont accessibles à partir de divers appareils clients par l'intermédiaire d'une interface client mince, comme un navigateur Web (p. ex. courriel sur le Web), ou d'une interface de programme. Le client ne gère pas et ne contrôle pas l'infrastructure infonuagique sous-jacente, notamment le réseau, les serveurs, les systèmes d'exploitation, le stockage ou même des capacités d'applications particulières, à l'exception possible de paramètres de configuration limités d'applications propres à un utilisateur. [NIST]
« Éditeur de ANS » : l'entité qui possède, exploite, maintient et distribue des solutions de ANS.

« Disponibilité de la solution » : le pourcentage de minutes pendant lequel la solution est opérationnelle au cours d'un mois.

« Documentation de la solution » : l'ensemble des manuels, livrets, guides d'utilisation et autres documents écrits en langage courant que l'entrepreneur doit fournir au Canada, conformément au contrat, et qui sera utilisé avec la solution.

« Solution », « solution de logiciel-service, de logiciel comme service ou de ANS » : l'application logicielle livrée selon un modèle de distribution de logiciels-service dans lequel un entrepreneur de services applicatifs ou un entrepreneur de services infonuagique met à la disposition des clients des applications logicielles hébergées de manière centralisée sur Internet, permettant ainsi l'accès à la solution mise à jour et actualisée, aux services de soutien technique, à l'infrastructure de technologie de l'information sécurisée physiquement et électroniquement, le tout compris dans le service d'abonnement.

Les « spécifications » désignent la description des exigences essentielles, fonctionnelles ou techniques liées aux services de l'annexe F – Accord sur les niveaux de services, y compris les procédures permettant de déterminer si les exigences ont été respectées.

La « soumission » désigne les documents que présente le soumissionnaire en réponse à la demande de propositions (DP).

Le « sous-traitant ultérieur » désigne la personne physique ou morale, l'autorité publique, l'organisme ou une autre organisation effectuant le traitement des données personnelles au nom d'un contrôleur des données.

Le terme « entrepreneur » désigne la personne ou l'entité (ou dans le cas d'une coentreprise, les personnes ou les entités) qui présente une soumission en réponse à la demande de proposition (DP) publiée par le Canada. Le terme ne comprend pas la société mère, les filiales ou autres affiliées d'entrepreneur, ni ses sous-traitants.

Les « droits d'utilisation » signifient qu'on accorde l'accès à une solution et son utilisation, ce qu'on désigne parfois sous le nom de licence d'abonnement.

L'« utilisateur » est toute personne, ou tout processus système agissant au nom d'une personne, que le Canada autorise à accéder aux services.

Le « revendeur de produits à valeur ajoutée » ou « RVA » désigne un entrepreneur qui est une filiale, un partenaire, un revendeur de produits à valeur ajoutée ou un autre distributeur de ANS. Le RVA n'inclut pas un éditeur de logiciels, un éditeur de ANS ou un entrepreneur de services infonuagiques (FSI) qui est également un éditeur de ANS.

« travaux » désigne les activités, services, biens, équipements, choses et objets que l'entrepreneur doit exécuter, livrer ou fournir en vertu du contrat.

« Appareils technologiques en milieu de travail » : les ordinateurs de bureau, les postes de travail mobiles, comme les ordinateurs portables et les tablettes, les téléphones intelligents, les téléphones, les périphériques et les accessoires, comme les moniteurs, les claviers, les souris, les dispositifs audio et les dispositifs internes et externes de stockage, notamment les clés USB, les cartes mémoire, les disques durs externes, et les CD et DVD inscriptibles.

ANNEXE « A » – ÉNONCÉ DES BESOINS

ANNEXE A - ÉNONCÉ DES BESOINS

1. Exigence gouvernementale

Emploi et Développement social Canada (EDSC), un ministère du gouvernement du Canada (Canada), a besoin d'un Système d'application de continuité des activités et de gestion des urgences (SACAGU). Le SACAGU doit être fourni comme logiciel en tant que service (SaaS) sur un nuage public capable de traiter des données de niveau Protégé B, ce qui facilitera la création, la surveillance, la gestion et la consolidation de l'information sur la gestion des urgences (p. ex., les plans) et des données (p. ex., coordonnées) dans les quatre piliers de la gestion des urgences (figure 1 ci-dessous).

Le SACAGU exige que les secteurs fonctionnels suivants, d'importance égale, appuient les quatre piliers de la gestion des urgences :

- Gestion de la continuité des activités
- Gestion de la continuité des activités de la TI
- Gestion d'urgence et d'évacuation dans les immeubles
- Gestion des crises et des urgences

Sans SACAGU, les éléments susmentionnés représentent un défi logistique pour une organisation ayant la taille et la complexité d'EDSC.

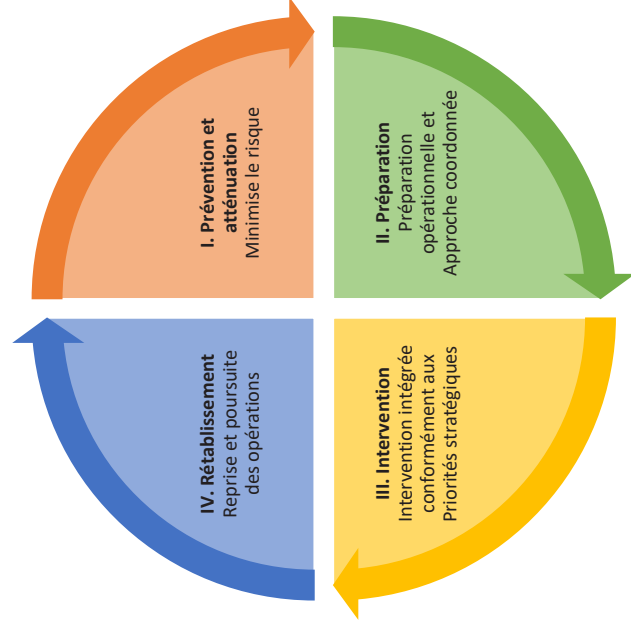
À titre de ministère fédéral, EDSC compte environ 30 000 employés, souvent gérés virtuellement, dans environ 490 emplacements au Canada, qui travaillent dans plusieurs secteurs d'activité. La Direction générale de l'innovation, de l'information et de la technologie (DGIIIT) d'EDSC fournit des services d'information et de technologie à EDSC, incluant les applications opérationnelles qui supportent et simplifient les méthodes de travail, l'accès aux données et le traitement de millions de transactions relatives aux prestations afin de répondre aux besoins des canadiens. De façon continue, EDSC soutient plus de 400 applications de GI-TI pour offrir des prestations dont dépendent des millions de canadiens, dont plus de 100 permettent des services essentiels. Cette complexité entraîne des problèmes d'exactitude des rapports et des données ainsi que de la difficulté à déterminer l'état de préparation d'EDSC (p. ex., exercice de surveillance et achèvement du plan d'urgence).

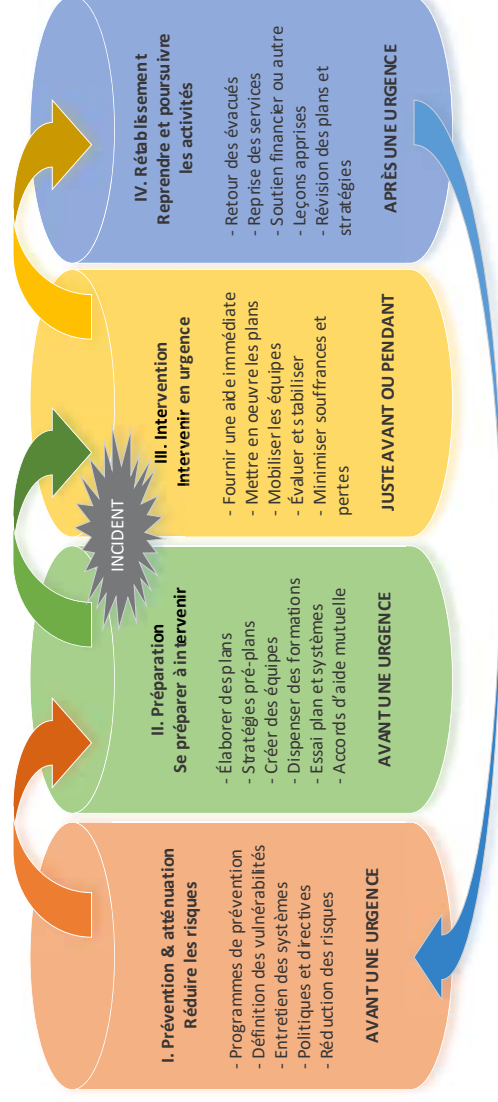
La consolidation de l'information et des données sur la gestion des urgences d'EDSC (c.-à-d. une base de données relationnelle) augmentera la confiance d'EDSC dans la prise de décisions lors de situations d'urgence en améliorant les capacités de surveillance (p. ex., l'achèvement du plan), l'identification des interdépendances (p. ex., entre les programmes, les services, les systèmes de TI et leurs emplacements géographiques) et l'information et les données à jour.

EDSC a besoin d'accéder à l'information et aux données d'urgence, via SACAGU, pour coordonner et intervenir lors de situations d'urgence dans ses secteurs d'activité et de sa zone géographique. Pour ce faire, EDSC a besoin d'un système accessible à l'échelle du Canada qui assure une résilience contre les pannes de réseau.

La coordination et la surveillance de la préparation aux situations d'urgence d'EDSC (p. ex., achèvement du plan d'urgence et des exercices) font face aux mêmes défis liés à la répartition de l'effectif mentionnés ci-dessus. EDSC a besoin d'un système qui facilite la surveillance et le partage de l'information ainsi que la création de plans et de rapports normalisés à l'échelle du ministère.

Figure 1 : Cycle de gestion des urgences (I. Prévention, II. Préparation, III. Intervention, IV. Reprise)





2. But et priorités

Le SACAGU vise à simplifier les quatre secteurs fonctionnels de la gestion des urgences à EDSC en tenant compte des priorités suivantes :

- Disponibilité
- Automatisation
- Surveillance
- Exactitude des données
- Protection du personnel, des biens et des opérations en cas d'urgence.

Les principaux facteurs de réussite sont la préparation (p. ex. planification, mise à l'essai et surveillance) de la continuité des activités et de la reprise des services de TI ainsi que l'efficacité de la coordination et de la communication entre les nombreux intervenants dans la coordination d'une intervention ministérielle, régionale et locale en cas d'urgence.

État actuel

Présentement, les solutions déployées à EDSC offrant des fonctionnalités semblables à celles requises par le SACAGU sont disparates, ne partagent pas l'information entre elles et ne sont que partiellement automatisées. Plusieurs de ces outils se sont révélés efficaces, mais

ne répondent pas entièrement à tous les besoins d'EDSC. En remplacement, le SACAGU nécessitera la migration des ressources d'information du système actuel.

3. Buts et objectifs

L'objectif du SACAGU est de fournir aux utilisateurs d'EDSC à l'échelle du Canada un accès via une connexion Internet à un seul système automatisé qui gère les quatre piliers de la gestion des urgences.

Le SACAGU a pour but d'améliorer la capacité d'EDSC à maintenir la sûreté et la sécurité de ses employés et de ses clients, de continuer à offrir les programmes et services d'EDSC aux canadiens lors de situation d'urgence et de s'acquitter de ses responsabilités en vertu du [Plan fédéral d'intervention d'urgence](#) soutenant les canadiens lors d'urgence fédérale.

4. Échéancier de mise en œuvre du projet

Le SACAGU sera implanté en deux phases :

- Phase 1 : Fournir un accès initial à 20 utilisateurs principaux, une formation complète, la configuration des solutions/services, la migration des données existantes, la mise à l'essai et l'acceptation des services par le Canada.

Les utilisateurs principaux sont ceux qui seraient en mesure de former les autres futurs utilisateurs et de participer activement à la configuration/installation, aux tests et à la migration des actifs d'information de la solution.

- Phase 2 : Accès aux 2 980 autres utilisateurs, leur formation et déploiement complet.

5. Portée

Le SACAGU sera livré comme logiciel en tant que service (SaaS) qui répond le mieux à toutes les exigences énoncées dans le présent énoncé des besoins, y compris une conformité obligatoire aux contrôles de sécurité des technologies de l'information sélectionnés dans le document « [Profil de contrôle de sécurité du Canada pour les services de TI en nuage pour les niveaux Protégé B, Intégrité et disponibilité moyennes \(PBMM\)](#) » ci-joint. Il sera livré dans le nuage public et aura la capacité de traiter les données Protégé B. Pour en savoir plus sur la conformité à la sécurité des TI et le raisonnement justifiant la sélection des contrôles, consultez le diagramme des modèles de services informatiques en nuage à l'annexe C.

La portée du présent approvisionnement englobe :

- Le SACAGU, en tant que type de service SaaS;
- Les services professionnels requis pour les aspects susmentionnés de la mise en œuvre et du déploiement.

La portée fonctionnelle du SACAGU comprendra les éléments suivants :

1. Gestion de crise
2. Gestion de la continuité des activités
3. Planification de la reprise après sinistre
4. Planification de la reprise de la TI
5. Préparation aux situations d'urgence dans les immeubles
6. Essais et exercices
7. Communications d'urgence
8. Surveillance et production de rapports

Pour faciliter l'exécution du projet, le Canada exige que le soumissionnaire offre les services professionnels suivants :

1. Service de formation (approche de formation des formateurs)
Le Canada exige que le soumissionnaire retenu offre une formation suffisamment complète aux vingt premiers utilisateurs (considérés comme des utilisateurs principaux) d'EDSC, pour leur permettre d'exécuter des fonctions administratives, c.-à-d. configuration, migration des actifs informationnels existants, mise à l'essai, formation et déploiement des services auprès des 2 980 autres utilisateurs.
2. Services de configuration et de mise à l'essai
Le Canada exige que le soumissionnaire retenu fournisse des services professionnels pour la configuration, l'adaptation et la mise à l'essai du SACAGU.
3. Services de migration
Le Canada exige que le soumissionnaire retenu fournisse des services professionnels pour la migration des ressources d'information du Canada des anciens systèmes au SACAGU.
4. Services de déploiement

Le Canada exige que le soumissionnaire retenu fournisse des services professionnels pour le déploiement du SACAGU aux 2 980 autres utilisateurs.

6. Rôles du SACAGU

Le SACAGU servira quatre (4) principaux types de rôles, qui auront les capacités respectives suivantes :

1. **Administrateur du SACAGU** – dispose de tous les droits et privilèges :
 - a. incluant les sous-rôles de responsable et d'approuvateur du plan;
 - b. configure et gère les paramètres du système;

- c. gère l'accès au système pour les utilisateurs d'EDSC;
 - d. crée, gère et supprime l'information, les données et les flux de travail;
 - e. produit des rapports et effectue une surveillance à l'échelle du système;
2. **Coordonnateur du SACAGU** – ses privilèges d'accès au système sont limités selon son secteur d'activité :
- a. gère l'accès au système pour les utilisateurs d'EDSC dans un secteur opérationnel donné;
 - b. tient à jour les écrans du SACAGU pour son secteur d'activité;
 - c. crée, gère et supprime l'information, les données et les flux de travail;
 - d. produit des rapports et effectue un suivi pour son secteur d'activité.
3. **Contributeur du SACAGU** – ses privilèges d'accès au système sont limités selon son secteur d'activité :
- a. crée, modifie, gère et approuve les données, l'information et les flux de travail;
 - b. produit des rapports et effectue un suivi pour son secteur d'activité.
4. **Visualiseur du SACAGU** – dispose de privilèges d'accès au système en mode lecture-seulement et restreints en fonction du domaine d'activité ou du besoin de savoir :
- a. dispose seulement des droits de visionnement;
 - b. inclue un sous-rôle d'un membre du groupe de surveillance.

Les quatre types d'utilisateurs d'EDSC susmentionnés seront des représentants de divers secteurs, mais sans s'y limiter :

- Cadres d'EDSC
- Personnel d'urgence de l'immeuble
- Personnel du Centre national et des Centres régionaux des opérations d'urgence (CNOU)/(CROU)
- Bureaux régionaux de la sécurité
- Personnel de la gestion des incidents de TI
- Personnel de la santé et sécurité au travail
- Coordonnateurs de la continuité des activités et de la gestion des urgences

Les acronymes et les termes utilisés dans le présent document figurent aux Annexes A et B.

7. Exigences du SACAGU

7.1. Exigences obligatoires

7.1.1. Exigences relatives à la conformité de la sécurité

Les exigences de sécurité suivantes (MS1-MS14) doivent être respectées afin de démontrer la conformité à la sécurité des données jusqu'au niveau Protégé B.

Le soumissionnaire peut décider d'indiquer si les fournisseurs de composants SaaS de PaaS et d'IaaS ont déjà obtenu le statut (accord-cadre) d'un fournisseur de ces services infonuagiques au Canada, comprenant le niveau Protégé B – Moyen – Moyen (un accord-cadre, communément appelé « AC infonuagique du GC »). Dans un tel cas, joint à la proposition, le soumissionnaire doit présenter des preuves respectives obtenues des fournisseurs d'IaaS et de PaaS, telle que le nom du fournisseur respectif et le numéro de référence de son accord-cadre (voir l'exigence MS1).

Pour simplifier les réponses au tableau 1 ci-dessous, lorsqu'une exigence (ou une partie de l'exigence) est liée à une PaaS ou à une IaaS, le soumissionnaire peut simplement indiquer la référence au « AC infonuagique du GC » si ce DF couvre ce qui est demandé par l'exigence. Autrement, si le fournisseur de PaaS et d'IaaS du soumissionnaire n'a pas de « AC infonuagique du GC », la réponse doit être entièrement détaillée, comme le décrit le tableau ci-dessous.

Cependant, partout où dans les exigences il y a une composante de SaaS, le soumissionnaire doit démontrer sa conformité détaillée comme décrit dans le tableau ci-dessous.

Tableau 1. Exigences relatives à la conformité en matière de sécurité (données jusqu'au niveau Protégé B)

Numéro	Critère	Obligation d'information du soumissionnaire	Renvoi à la proposition du soumissionnaire
MS1	Assurance de tiers – Certifications et rapports Le soumissionnaire et tous les fournisseurs qui fournissent des composants de logiciel en tant que service (SaaS) disponibles sur le marché dans le cadre de la solution du soumissionnaire doivent se conformer aux exigences de sécurité sélectionnées dans le Profil de contrôle de sécurité du gouvernement du Canada pour les services de TI en nuage du gouvernement du Canada à la date de clôture des soumissions. Pour	Le soumissionnaire doit fournir la preuve des certifications de l'industrie suivantes pour le SaaS : i. ISO/IEC 27001:2013 ii. ISO/CEI 27017:2015 iii. ISO/CEI 27018:2019 iv. Contrôle de l'organisme de services de l'AICPA (SOC) 2 Type II	

Numéro	Critère	Obligation d'information du soumissionnaire	Renvoi à la proposition du soumissionnaire
	<p>chaque composante du SaaS disponible sur le marché qui est comprise dans la solution du soumissionnaire, le soumissionnaire et les fournisseurs, le cas échéant, doivent posséder les certifications de l'industrie suivantes pour démontrer leur conformité :</p> <ul style="list-style-type: none"> • Norme ISO/CEI 27001:2013 Technologies de l'information – Techniques de sécurité – Systèmes de management de la sécurité de l'information – Exigences; • Norme ISO/CEI 27017:2015 Technologies de l'information – Techniques de sécurité – Code de pratique des contrôles de sécurité de l'information fondé sur ISO/CEI 27002 pour les services du nuage; • ISO/IEC 27018:2019 Techniques de sécurité – Code de pratique pour la protection des renseignements personnels identifiables dans les nuages publics agissant comme processeurs de renseignements personnels identifiables; • Rapport de Contrôle de l'organisation des services de l'AICPA (American Institute of Certified Public Accountants) (SOC) 2 Type II pour les principes de confiance en matière de sécurité, de disponibilité, d'intégrité du traitement et de confidentialité. 	<p>Chaque certification doit :</p> <ol style="list-style-type: none"> Être valide à la date de soumission; Indiquer la dénomination sociale du sous-traitant proposé; Indiquer la date de la certification actuelle; Indiquer la liste des actifs, de l'infrastructure de l'entrepreneur et des lieux de service visés par le rapport de certification; Être émise par un tiers indépendant qualifié en vertu de l'AICPA ou de CPA Canada et/ou du régime de certification ISO et conforme à la norme de système qualité ISO/IEC 17020. <p>Le soumissionnaire doit également fournir les rapports de vérification connexes. Ces rapports de vérification doivent avoir été produits dans les 12 mois précédant le début du contrat proposé. La portée des rapports doit correspondre aux emplacements et aux services offerts par le SaaS proposé disponible sur le marché. Si la méthode découpée est utilisée pour exclure les organisations de sous-services comme l'hébergement de centres de données, le rapport d'évaluation de l'organisation de sous-services doit être inclus.</p> <p>Le rapport de vérification doit provenir d'un tiers indépendant qualifié en vertu du régime de certification de l'AICPA ou de CPA Canada et/ou ISO et conforme à la norme de système qualité ISO/IEC 17020.</p>	

Numéro	Critère	Obligation d'information du soumissionnaire	Renvoi à la proposition du soumissionnaire
		<p>En plus des exigences obligatoires précisées ci-dessus, le soumissionnaire peut fournir des preuves supplémentaires tirées des plans de sécurité du système, de la conception des systèmes d'information, de l'architecture du système d'information ou des documents qui fournissent une description complète du système qui démontrent la conformité avec le profil de contrôle de sécurité du GC pour les services de TI nuage du GC pour PBMIM.</p> <p>Pour tout fournisseur qui a complété le processus d'évaluation de la sécurité des TI (PES TI) du fournisseur de services informatiques du Centre canadien pour la cybersécurité (CCCS) pour le composant SaaS, au niveau Protégé B - Moyen - Moyen (PBMIM), le soumissionnaire doit fournir des documents confirmant que le fournisseur a complété le processus d'intégration, incluant : (i) une copie du plus récent rapport d'évaluation rempli et fourni par le gouvernement du Canada et (ii) une copie du plus récent rapport sommaire fourni par le gouvernement du Canada.</p> <p>Si le soumissionnaire n'a pas complété ce SAP TI, il doit indiquer s'il l'a officiellement demandé au CCCS et où il se trouve dans ce processus au moment de la soumission.</p> <p>Le soumissionnaire doit également fournir les noms des fournisseurs des composants IaaS et PaaS de la solution et les numéros de référence de leur accord-cadre de l'informatique en nuage du gouvernement du Canada respectif, s'ils l'ont obtenu du gouvernement du Canada.</p>	
MS2	Rôles et responsabilités pour la sécurité Le soumissionnaire doit avoir clairement défini les rôles et responsabilités liés aux contrôles de sécurité et aux	Les rôles et responsabilités du soumissionnaire pour : <ol style="list-style-type: none"> la gestion de comptes; 	

Numéro	Critère	Obligation d'information du soumissionnaire	Renvoi à la proposition du soumissionnaire
	caractéristiques des services entre le soumissionnaire, ses sous-traitants et le Canada dans la chaîne d'approvisionnement de la solution infonuagique proposée et du Canada.	<ul style="list-style-type: none"> ii. la protection des frontières; iii. la sauvegarde des actifs et des systèmes d'information; iv. la gestion des incidents; v. la surveillance du système; vi. la gestion des vulnérabilités. <p>Une liste contenant des renseignements sur les tiers (p. ex. filiales, sous-traitants, etc.) qui font partie de sa solution.</p> <p>Aux fins de la présente exigence, un fournisseur qui n'est qu'un fournisseur de biens pour le soumissionnaire, mais qui n'exécute aucune partie de la chaîne d'approvisionnement n'est pas considéré comme un tiers.</p>	
MSS	<p>Isolement de la protection des données</p> <p>La solution proposée doit isoler les données au Canada dans un centre de données approuvé.</p> <p>Aux fins de la présente demande de soumissions, un centre de données approuvé est défini comme suit :</p> <ul style="list-style-type: none"> i. Un centre de données géographiquement situé au Canada; ii. Un centre de données qui satisfait à toutes les exigences de sécurité et à toutes les certifications identifiées. <p>Exigences relatives aux installations du centre de données :</p> <p>La solution proposée doit garantir que des mesures de sécurité sont mises en œuvre pour protéger les installations de TI et les actifs du système d'information sur lesquels les données du Canada sont stockées et</p>	<p>La documentation du système ou la documentation technique qui décrit en détails les mesures de sécurité, notamment les politiques, les processus et les procédures qui sont mis en œuvre pour protéger les installations de TI et les actifs du système d'information sur lesquels les données du gouvernement du Canada sont stockées et traitées contre toutes formes de falsification, de perte, de dommage et de saisie, et qui est basé sur une approche de prévention-détection-intervention-reprise de la sécurité physique.</p>	

Numéro	Critère	Obligation d'information du soumissionnaire	Renvoi à la proposition du soumissionnaire
	<p>traitées contre toutes les formes de falsification, de perte, de dommage et de saisie, et qui est basé sur une approche de prévention-détection-intervention-reprise de la sécurité physique. Les mesures de protection physique doivent être appliquées conformément aux contrôles de sécurité de la protection physique et de l'environnement (PE), de la maintenance (MA) et de la protection des médias (MP) décrits dans le ITSG-33</p> <p>Profil des mesures de sécurité pour les services informatiques du gouvernement du Canada fondés sur le nuage pour PBMM et la mise en pratique des directives et des normes sur la sécurité physique de la Gendarmerie royale du Canada (GRC).</p> <p>Il s'agit à tout le moins des éléments suivants :</p> <ul style="list-style-type: none"> i. capacités de redondance et de récupération suffisantes au sein et dans ses installations informatiques, géographiquement disparates et de sorte que la perte d'un centre de données n'empêche pas la récupération des données dans l'entente concernant le niveau de service prescrit; ii. gestion appropriée des supports informatiques; iii. maintenance contrôlée des systèmes d'information et de leurs composants pour protéger leur intégrité et assurer leur disponibilité en continue; iv. accès contrôlé aux périphériques de sortie des systèmes d'information pour empêcher l'accès non autorisé aux données du Canada; v. limiter l'accès physique aux actifs des systèmes d'information aux employés et aux contracteurs autorisés en fonction de leur poste ou de leur rôle 		

Numéro	Critère	Obligation d'information du soumissionnaire	Renvoi à la proposition du soumissionnaire
	<p>et au principe du besoin de savoir, qui est validé par deux formes d'identification;</p> <ul style="list-style-type: none"> vi. escorter les visiteurs et surveiller leur activité; vii. maintenir un registre d'accès physique; viii. contrôler et gérer les dispositifs d'accès physique; ix. mettre en application les mesures de protection des données du gouvernement du Canada dans d'autres sites de travail alternatifs (p. ex., lieux de télétravail); x. enregistrer et surveiller tout accès physique aux centres de données et tout accès logique aux composants des systèmes d'information qui hébergent les données du Canada, en combinant les registres d'accès et la vidéosurveillance dans toutes les zones délicates et des mécanismes de détection des intrusions. 		
MS4	<p>Séparation des données</p> <p>La solution proposée doit comprendre des contrôles visant à assurer une isolation appropriée des ressources de manière à ce que les ressources d'information ne soient pas amalgamées avec des données d'autres locataires pendant leur utilisation, leur stockage ou leur transit, et dans tous les aspects de la solution du soumissionnaire et de la fonctionnalité et de l'administration du système de l'infrastructure. Cela comprend la mise en place de contrôles d'accès et l'application d'une séparation logique ou physique appropriée pour soutenir :</p>	Documents démontrant comment le soumissionnaire se conforme aux exigences.	

Numéro	Critère	Obligation d'information du soumissionnaire	Renvoi à la proposition du soumissionnaire
	<ul style="list-style-type: none"> i. La séparation entre l'administration interne du soumissionnaire et les ressources utilisées par ses clients; ii. La séparation des ressources des clients dans des environnements à locaux multiples afin d'empêcher un consommateur malveillant ou compromis d'avoir des conséquences sur le service ou les données d'un autre. 		
M55	<p>Protection des données</p> <p>La solution proposée doit permettre au gouvernement du Canada de stocker et de protéger ses données inactives, notamment les données sauvegardées ou conservées à des fins de redondance dans les limites géographiques du Canada.</p> <p>Ceci inclus :</p> <ul style="list-style-type: none"> i. identifier et fournir au gouvernement du Canada une liste à jour des emplacements physiques, comprenant la ville, où peut se trouver les données canadiennes au Canada pour chaque centre de données qui sera utilisé pour fournir les services. identifier quelles parties des services sont fournies à partir de l'extérieur du Canada, y compris tous les emplacements où les données sont stockées et traitées et d'où ils gèrent le service. ii. s'assurer qu'il soit impossible de trouver des données précises sur un client dans nos médias sur les supports physiques; 	<p>Respectivement pour les deux premiers éléments énumérés :</p> <ul style="list-style-type: none"> i. Des captures d'écran du centre de données disponible où les centres de données canadiens figurent sur la liste des disponibilités; ii. Une liste ou carte indiquant l'emplacement géographique des centres de données au Canada. 	

Numéro	Critère	Obligation d'information du soumissionnaire	Renvoi à la proposition du soumissionnaire
	iii. utiliser le cryptage pour s'assurer qu'aucune donnée n'est inscrite sur un disque non-encrypté.		
MS6	<p>Installations du centre des données</p> <p>La solution proposée doit inclure des mesures de sécurité pour la protection des installations de TI, les données et les actifs du système d'information sur lequel les données du Canada sont stockées et traitées contre toutes formes de falsification, de perte, de dommage et de saisie, qui est basée sur un système de prévention, de détection, d'intervention et de reprise de la sécurité matérielle. Les mesures de protection physique doivent être appliquées conformément ou utiliser une approche adéquate axée sur le risque et harmonisée aux contrôles de sécurité physique et aux pratiques de la Norme opérationnelle sur la sécurité matérielle du Conseil du Trésor (https://www.tbs-sct.gc.ca/pol/doc-fra.aspx?id=12329). Les mesures de sécurité requises en vertu de cette norme comprennent, à tout le moins, ce qui suit :</p> <ul style="list-style-type: none"> i. capacités suffisantes de redondance et de récupération des données dans ses installations de TI et entre celles-ci. Elles doivent être géographiquement disparates, de sorte que la perte d'un centre de données n'empêche pas la récupération des données dans l'entente concernant le niveau de service prescrit; ii. manipulation appropriée des supports de TI; 	<p>La documentation sur le système ou la documentation technique décrivant en détail les mesures de sécurité, notamment les politiques, les processus et les procédures, qui sont mis en œuvre pour protéger les installations de TI, les données et les biens des systèmes d'information dans lesquels les données du Canada sont stockées et traitées contre toute forme de falsification, de perte, de dommage et de saisie. Ces mesures reposent sur une approche de prévention, de détection, d'intervention et de reprise de la sécurité matérielle.</p>	

Numéro	Critère	Obligation d'information du soumissionnaire	Renvoi à la proposition du soumissionnaire
	<ul style="list-style-type: none"> iii. maintenance contrôlée des systèmes d'information et de leurs composants pour protéger leur intégrité et assurer leur disponibilité continue; iv. accès contrôlé aux périphériques de sortie des systèmes d'information pour empêcher l'accès non autorisé aux données du Canada; v. accès physique limité aux actifs des systèmes d'information aux employés et aux répondants autorisés en fonction de leur poste ou de leur rôle et du principe besoin de savoir et qui est validé par deux formes d'identification; vi. escorter les visiteurs et surveiller leur activité; vii. maintenir un registre d'accès physique; viii. contrôler et gérer les dispositifs d'accès physique; ix. mettre en application les mesures de protection des données du gouvernement du Canada dans d'autres sites de travail alternatifs (p. ex., lieux de télétravail); x. enregistrer et surveiller tout accès physique aux centres de données et de tout accès logique aux composants des systèmes d'information qui hébergent les données du Canada, en combinant les registres d'accès et la vidéosurveillance dans toutes les zones délicates et les mécanismes de détection des intrusions. 		
MS7	Respect de la vie privée dès la conception La solution proposée doit :	Description du cycle de développement des logiciels du soumissionnaire	

Numéro	Critère	Obligation d'information du soumissionnaire	Renvoi à la proposition du soumissionnaire
	<ul style="list-style-type: none"> i. Comprendre un cycle de développement de logiciels conforme à la norme ISO 27032 et intégrant la protection de la vie privée dès la conception; ii. se conformer au Cadre de gestion de la protection des renseignements personnels et aux exigences précisées dans la Norme ISO 29100; iii. Respecter les sept principes fondamentaux de la protection de la vie privée dès la conception (voir https://www.ipc.on.ca/wp-content/uploads/Resources/7foundationalprinciples.pdf). 	<p>Une description du cadre de gestion de la protection des renseignements personnels du soumissionnaire, y compris les principes régissant la protection des renseignements personnels et un aperçu des politiques de protection des renseignements personnels du soumissionnaire</p>	
MS8	<p>Gestion de l'accès</p> <p>La solution proposée doit satisfaire aux exigences de sécurité suivantes en matière de gestion de l'accès :</p> <ul style="list-style-type: none"> i. Gérer et surveiller l'accès à la solution, y compris à l'infrastructure sous-jacente, pour s'assurer que toutes les interfaces de service dans un environnement multi locataire sont protégées contre l'accès non autorisé, y compris celles qui sont utilisées pour héberger les services du GC; ii. Restreindre et minimiser l'accès aux services et aux actifs d'information du Canada aux seuls dispositifs autorisés et aux utilisateurs finaux qui ont explicitement besoin d'y avoir accès; iii. Appliquer et vérifier les autorisations d'accès aux services et aux actifs d'information; iv. Limiter les accès aux interfaces de service qui hébergent les actifs et les actifs d'information 	<p>Documentation du système ou livre blanc décrivant les politiques, les processus et les procédures utilisés pour gérer la gestion de l'accès.</p>	

Numéro	Critère	Obligation d'information du soumissionnaire	Renvoi à la proposition du soumissionnaire
	<p>uniquement aux utilisateurs identifiés, authentifiés et autorisés, ainsi qu'aux dispositifs et aux processus (ou services);</p> <p>v. Mettre en œuvre des politiques sur les mots de passe afin de protéger les informations d'identification contre toute compromission d'attaques en ligne ou hors ligne et pour détecter ces attaques en enregistrant et en surveillant des événements comme (i) l'utilisation réussie des informations d'identité (ii) l'utilisation inhabituelle des informations d'identité et (iii) l'accès et l'exfiltration de la base de données des mots de passe, conformément à la norme ITSP 30.031 V3 (ou versions subséquentes) du CST (https://www.cyber.gc.ca/fr/orientation/guide-sur-lauthentification-des-utilisateurs-dans-les-systemes-de-technologie-de);</p> <p>vi. Mettre en œuvre des mécanismes d'authentification multifactorielle pour authentifier les utilisateurs finaux (niveau 2 seulement) avec accès, conformément à la politique ITSP.30.031 V3 (ou versions subséquentes) du CST (https://www.cyber.gc.ca/fr/orientation/guide-sur-lauthentification-des-utilisateurs-dans-les-systemes-de-technologie-de);</p> <p>vii. Mettre en œuvre des mécanismes de contrôle de l'accès fondés sur les rôles pour attribuer des privilèges qui constituent la base de l'application de l'accès aux actifs et aux actifs d'information;</p> <p>viii. Définir et mettre en œuvre la séparation des tâches pour atteindre, au minimum, la séparation des rôles de gestion des services et d'administration des rôles de support du système d'information, des</p>		

Numéro	Critère	Obligation d'information du soumissionnaire	Renvoi à la proposition du soumissionnaire
	<p>rôles de développement des rôles opérationnels et des rôles de gestion des accès à d'autres rôles opérationnels;</p> <p>ix. Respecter les principes du droit d'accès minimal et du besoin de savoir au moment de donner accès aux services et aux actifs, et aux actifs d'information;</p> <p>x. Mettre en place des contrôles d'accès aux objets stockés et politiques d'autorisation granulaires pour autoriser ou limiter l'accès</p> <p>xi. Utiliser des points d'extrémité renforcés par la sécurité (p. ex., ordinateurs, appareils d'utilisateur final, serveurs intermédiaires, etc.) configurés pour une fonctionnalité minimale (p. ex., point d'extrémité dédié qui n'offre pas de navigation sur Internet ou d'accès ouvert à la messagerie) pour assurer le soutien et l'administration des Services et Infrastructure de l'entrepreneur;</p> <p>xii. Mettre en œuvre un processus automatisé pour vérifier périodiquement, au minimum, les actions de création, de modification, d'activation, de désactivation et de suppression de comptes;</p> <p>xiii. Au moment de la cessation d'emploi, résilier ou révoquer les informations d'authentification et d'accès associés à tout membre du personnel.</p>		
MS9	<p>Fédération de l'identité</p> <p>La solution proposée doit appuyer l'intégration de l'identité fédérée, notamment :</p> <p>i. Mettre en œuvre des mécanismes d'authentification multifactorielle pour authentifier</p>	La documentation du système ou la documentation technique décrivant et détaillant les mesures de sécurité, y compris les politiques, processus et procédures mis en œuvre pour la protection de la fédération de l'identité.	

Numéro	Critère	Obligation d'information du soumissionnaire	Renvoi à la proposition du soumissionnaire
	<p>les utilisateurs au moyen d'un accès privilégié, conformément à la politique ITSP.30.031 V3 du CST (ou versions subséquentes) https://www.cyber.gc.ca/fr/orientation/guide-sur-l-authentification-des-utilisateurs-dans-les-systemes-de-technologie-de);</p> <p>ii. Le soutien du langage de balisage des assertions de sécurité (SAML) 2.0 et l'OpenID Connect 1.0 où les justificatifs d'identité et l'authentification de l'utilisateur final aux services infonuagiques sont sous le contrôle exclusif du Canada;</p> <p>iii. La capacité d'associer des identifiants uniques au Canada (p. ex., un identifiant unique au Canada, une adresse électronique au Canada, etc.) avec le ou les compte(s) d'utilisateur de service informatique en nuage correspondants.</p>		
MS10	<p>Protection des points d'extrémité</p> <p>La solution proposée doit comprendre la mise en œuvre, la gestion et la surveillance des points d'extrémité a sécurité renforcée afin de prévenir les attaques et abus conformément aux lignes directrices de configuration reconnues par l'industrie, comme celles du NIST 800-123 (Guide to General Server Security), le Center for Internet (CIS) ou une norme équivalente approuvée par écrit par le Canada.</p>	<p>Documentation du système ou documentation technique décrivant et détaillant les mesures de sécurité, y compris les politiques, processus et procédures mis en œuvre pour la protection des points d'extrémité.</p>	

Numéro	Critère	Obligation d'information du soumissionnaire	Renvoi à la proposition du soumissionnaire
MS11	<p>Développement sécurisé</p> <p>La solution proposée doit comprendre la mise en œuvre d'un cycle de vie de développement de logiciels et de systèmes qui applique les principes d'ingénierie de sécurité des systèmes d'information tout au long du cycle de vie du système d'information et lors du développement de logiciels, de sites Web et de services, et qui est conforme aux normes et aux pratiques exemplaires de l'industrie, notamment :</p> <ul style="list-style-type: none"> i. NIST ii. ASI iii. ITSG-33 iv. SAFECode ou v. Normes de l'Open Web Application Security Project (OWASP) telles que l'Application Security Verification Standard (ASVS) ou une norme équivalente approuvée par écrit par le Canada. 	Documentation du système ou documentation technique décrivant et détaillant les mesures de sécurité, y compris les politiques, processus et procédures mis en place pour le développement sécurisé.	
MS12	<p>Gestion à distance de l'entrepreneur</p> <p>La solution proposée doit être en mesure de gérer et de surveiller l'administration à distance de la solution du soumissionnaire qui sert à héberger les services du gouvernement du Canada et de prendre des mesures raisonnables pour :</p> <ul style="list-style-type: none"> i. Mettre en œuvre des mécanismes d'authentification multi facteur pour authentifier les utilisateurs d'accès à distance, conformément à la politique ITSP.30.031 V3 du 	Documentation du système ou documentation technique décrivant et détaillant les mesures de sécurité, y compris les politiques, processus et procédures mis en œuvre pour la gestion à distance de l'entrepreneur	

Numéro	Critère	Obligation d'information du soumissionnaire	Renvoi à la proposition du soumissionnaire
	<p>CST (ou versions subséquentes) (https://www.cyber.gc.ca/fr/orientation/guide-sur-lauthentification-des-utilisateurs-dans-les-systemes-de-technologie-de);</p> <p>ii. Utiliser des mécanismes cryptographiques approuvés par le Centre de la sécurité des télécommunications du Canada pour protéger la confidentialité des sessions d'accès à distance;</p> <p>iii. Acheminer tous les accès à distance par des points de contrôle d'accès contrôlés, surveillés et vérifiés;</p> <p>iv. Débrancher ou désactiver rapidement les connexions non autorisées de gestion ou d'accès à distance;</p> <p>v. Autoriser l'exécution à distance des commandes privilégiées et l'accès à distance des informations relatives à la sécurité.</p>		
MS13	<p>Fuite d'information</p> <p>Le processus proposé en cas d'incident de fuite d'information doit être harmonisé avec le guide ITSG-33, Contrôle de sécurité pour l'intervention en cas de fuite d'information IR-9.</p>	Documentation du système ou documentation technique décrivant et détaillant les mesures de sécurité, y compris les politiques, les processus et les procédures qui sont mis en œuvre pour la protection contre la fuite d'information.	
MS14	<p>Protection cryptographique</p> <p>La solution proposée doit :</p> <p>i. Configurer toute cryptographie utilisée pour mettre en œuvre des mesures de protection de la confidentialité ou de l'intégrité ou utilisée dans le</p>	Documentation du système ou documentation technique décrivant et détaillant les mesures de sécurité, y compris les politiques, processus et procédures mis en œuvre pour assurer la protection cryptographique	

Numéro	Critère	Obligation d'information du soumissionnaire	Renvoi à la proposition du soumissionnaire
	<p>cadre d'un mécanisme d'authentification (p. ex., 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) ainsi qu'aux tailles et périodes cryptographiques des clés cryptographiques;</p> <p>ii. Utiliser des algorithmes cryptographiques ainsi que des tailles de clés cryptographiques et des périodes cryptographiques qui ont été validés par le Programme de validation des algorithmes cryptographiques (http://csrc.nist.gov/groups/STM/cavp/ - en anglais seulement) et qui sont précisés dans le document ITSP.40.111, Algorithmes cryptographiques pour les renseignements non classifiés, Protégé A et Protégé B, ou les versions subséquentes (https://cyber.gc.ca/fr/orientation/algorithmes-cryptographiques-pour-linformation-non-classifiee-protege-et-protege-b);</p> <p>iii. S'assurer que la cryptographie validée selon la norme FIPS 140 est utilisée lorsque le chiffrement est requis et qu'elle est mise en œuvre, configurée et exploitée dans un module cryptographique validé par le Programme de validation des modules cryptographiques (https://cyber.gc.ca/fr/programme-de-validation-des-modules-cryptographiques-pvmc) en mode approuvé ou autorisé afin d'assurer un degré élevé de certitude que le module cryptographique validé selon la norme FIPS 140-2 fournit les services de sécurité attendus de la manière prévue;</p>		

Numéro	Critère	Obligation d'information du soumissionnaire	Renvoi à la proposition du soumissionnaire
	iv. S'assurer que tous les modules FIPS 140-2 utilisés sont certifiés actifs, à jour et valides. Les produits conformes à la norme FIPS 140 auront des numéros de certificat.		

7.1.2 Exigences fonctionnelles – Obligatoires

Tableau 2 – Exigences fonctionnelles obligatoires

ID	Exigence	Justification
M1	Le système proposé par le soumissionnaire doit être une solution infonuagique de logiciel en tant que service (SaaS).	Le soumissionnaire doit démontrer sa conformité au moyen de documents techniques et d'autres moyens de preuve, comme la saisie d'écran.
M2	Le système logiciel proposé par le soumissionnaire doit être fonctionnel de façon équivalente dans les deux langues officielles du Canada (anglais et français) et doit permettre aux utilisateurs de travailler dans la langue officielle canadienne de leur choix.	Le soumissionnaire doit démontrer sa conformité en documentant sa capacité de répondre aux exigences, en utilisant des saisies d'écran ou des documents techniques ou d'utilisateur final pour compléter ses réponses.
M3	Le système proposé par le soumissionnaire doit permettre un accès simultané par 2 000 utilisateurs d'EDSC.	Le soumissionnaire doit démontrer sa conformité en utilisant des saisies d'écran (« écran d'impression » ou similaire) et/ou d'autres types de documents/données techniques ou d'utilisateur final qui démontrent clairement cette capacité.
M4	Le système proposé par le soumissionnaire doit pouvoir prendre en charge au moins 3 000 utilisateurs d'EDSC.	Le soumissionnaire doit démontrer sa conformité en utilisant des saisies d'écran ou des documents techniques ou d'utilisateur final qui démontrent clairement cette capacité.

ID	Exigence	Justification
M5	Le système proposé par le soumissionnaire doit fournir une capacité de gestion des documents et de l'information électroniques (p. ex., stockage, recherche, extraction et gestion des documents), organisée de manière hiérarchique (p. ex., par région, direction générale, direction).	Le soumissionnaire doit démontrer sa conformité en documentant sa capacité de répondre aux exigences, en utilisant des saisies d'écran ou des documents techniques ou d'utilisateur final pour compléter ses réponses.
M6	Le système proposé par le soumissionnaire doit offrir une capacité dans toutes les catégories suivantes : 1. Gestion de la continuité des activités; 2. Gestion de la reprise de la TI; 3. Gestion des urgences et évacuations des immeubles (équipes et plans d'urgences de l'immeuble); 4. Gestion des urgences; 5. Gestion de crise;	Le soumissionnaire doit démontrer sa conformité en documentant sa capacité de répondre aux exigences, en utilisant des saisies d'écran ou des documents techniques ou d'utilisateur final pour compléter ses réponses.
M7	Le système proposé par le soumissionnaire doit permettre la création, la gestion et l'approbation de plans de continuité des activités (PCA) intégrés pour les services au niveau ministériel, ce qui comprend le cumul des plans de continuité des activités à plusieurs niveaux organisationnels d'EDSC (p. ex., PCA au niveau régional, au niveau des directions générales, des directions et des divisions).	Le soumissionnaire doit démontrer sa conformité en documentant sa capacité de répondre aux exigences, en utilisant des saisies d'écran ou des documents techniques ou d'utilisateur final pour compléter ses réponses.
M8	Le système proposé par le soumissionnaire doit être disponible : 1. À l'échelle du Canada 2. À l'aide d'une connexion à un réseau câblé et sans fil; 3. Par le biais d'un ordinateur de bureau et d'appareils mobiles (p. ex., par le biais d'un navigateur Web mobile ou d'une application mobile)	Le soumissionnaire doit démontrer sa conformité en documentant sa capacité de répondre aux exigences, en utilisant des saisies d'écran ou des documents techniques ou d'utilisateur final pour compléter ses réponses.
M9	Le système proposé par le soumissionnaire doit permettre de créer, de modifier, de remplir, d'enregistrer et de gérer	Le soumissionnaire doit démontrer sa conformité en documentant sa capacité de répondre aux exigences, en utilisant des saisies d'écran ou des documents

ID	Exigence	Justification
M10	<p>des questionnaires (p. ex., questionnaire d'analyse des répercussions sur les activités) et des listes de vérification.</p> <p>Le système proposé par le soumissionnaire doit fournir une capacité de gestion du flux de travail, notamment :</p> <ol style="list-style-type: none"> 1. Permettre aux utilisateurs du SACAGU : <ol style="list-style-type: none"> i. de créer, assigner, réassigner et supprimer des tâches de flux de travail, ii. de créer, démarrer, retirer, supprimer, compléter les flux de travail, iii. de visualiser les flux et les tâches actifs, iv. d'établir des délais de présentation des flux de travail (ponctuels ou planifiés) pour toute tâche; v. de surveiller les flux de travail et d'en produire des rapports. 2. Exécuter automatiquement des flux de travail des documents électroniques 	<p>techniques ou d'utilisateur final pour compléter ses réponses.</p> <p>Le soumissionnaire doit démontrer sa conformité en documentant sa capacité de répondre aux exigences, en utilisant des saisies d'écran ou des documents techniques ou d'utilisateur final pour compléter ses réponses.</p>
M11	<p>Le système proposé par le soumissionnaire doit offrir aux administrateurs du SACAGU et aux coordonnateurs du SACAGU la capacité de gérer le contrôle de l'accès des utilisateurs (y compris la protection des renseignements personnels) et les paramètres d'autorisation.</p>	<p>Le soumissionnaire doit démontrer sa conformité en documentant sa capacité de répondre aux exigences, en utilisant des saisies d'écran ou des documents techniques ou d'utilisateur final pour compléter ses réponses.</p>
M12	<p>Les paramètres de confidentialité du système proposés par le soumissionnaire doivent permettre de restreindre la consultation des données sur les employés, selon la structure organisationnelle (c.-à-d. que les gestionnaires ne devraient voir que les données sur les employés des personnes affectées à leur unité de travail).</p>	<p>Le soumissionnaire doit démontrer sa conformité en documentant sa capacité de répondre aux exigences, en utilisant des saisies d'écran ou des documents techniques ou d'utilisateur final pour compléter ses réponses.</p>

ID	Exigence	Justification
M13	<p>Le système proposé par le soumissionnaire doit offrir une capacité de production de rapports qui comprend tous les éléments suivants :</p> <ol style="list-style-type: none"> 1. Création de rapports spéciaux en extrayant des données de n'importe quel champ de base de données. 2. 3. Personnalisation des rapports 3. 2. Création et gestion de modèles de rapports (retrait, modification et suppression) 4. Création de rapports programmés 	<p>Le soumissionnaire doit démontrer sa conformité en documentant sa capacité de répondre aux exigences, en utilisant des saisies d'écran ou des documents techniques ou d'utilisateur final pour compléter ses réponses.</p>
M14	<p>Le système proposé par le soumissionnaire doit permettre de produire des documents et des rapports électroniques imprimables.</p>	<p>Le soumissionnaire doit démontrer sa conformité en documentant sa capacité de répondre aux exigences, en utilisant des saisies d'écran ou des documents techniques ou d'utilisateur final pour compléter ses réponses.</p>
M15	<p>Le système proposé par le soumissionnaire doit sauvegarder quotidiennement tous les justificatifs d'identité, données et fichiers des utilisateurs d'EDSC (p. ex., rapports de vérification, documents, listes de personnes-ressources) dans un système de sauvegarde stocké dans un centre de données situé à un endroit différent du centre de données principal. Le centre de données secondaire doit être situé au Canada.</p>	<p>Le soumissionnaire doit démontrer sa conformité en documentant sa capacité de répondre aux exigences, en utilisant des saisies d'écran ou des documents techniques ou d'utilisateur final pour compléter ses réponses.</p>
M16	<p>Le système proposé par le soumissionnaire doit satisfaire à la Norme de l'UE¹ (EN 301 549), sections 5, 7, 9 et 12.</p>	<p>Le soumissionnaire doit démontrer sa conformité en incluant à sa soumission une évaluation officielle de la conformité, par exemple, dans l'ordre de préférence du Canada :</p> <ul style="list-style-type: none"> - Rapport de conformité à l'accessibilité (RCA) d'un évaluateur tiers accrédité.

ID	Exigence	Justification
		<ul style="list-style-type: none"> - Modèle d'accessibilité volontaire des produits (VPAT) par un évaluateur tiers accrédité. - VPAT, autoévalué. <p>¹Remarque : Dans la norme de l'UE, il y a un chevauchement avec la norme WCAG 2.1. Au minimum, la solution du soumissionnaire doit respecter les WCAG 2.1 aux niveaux A et AA.</p> <p>Le soumissionnaire peut compléter sa justification en fournissant toute autre preuve, capture d'écran ou documentation technique, acceptée par l'industrie.</p>
M17	Le système proposé par le soumissionnaire doit permettre de fournir des avis aux utilisateurs avant d'accorder l'accès et doit permettre aux utilisateurs de configurer le message de notification selon leurs besoins.	Le soumissionnaire doit démontrer sa conformité en documentant sa capacité de répondre aux exigences, en utilisant des saisies d'écran ou des documents techniques ou d'utilisateur final pour compléter ses réponses.

7.1.3 Exigences non fonctionnelles – obligatoires

Tableau 3 – Exigences non fonctionnelles obligatoires

ID	Exigence	Justification
M18	Le système proposé par le soumissionnaire doit permettre d'identifier et d'authentifier de façon unique les connexions à partir d'appareils externes et d'autoriser les appareils avant de permettre la connectivité.	Le soumissionnaire doit démontrer sa conformité en documentant sa capacité de répondre aux exigences, en utilisant des saisies d'écran ou des documents techniques ou d'utilisateur final pour compléter ses réponses.

ID	Exigence	Justification
M19	Le système proposé par le soumissionnaire doit afficher toutes les tentatives d'ouverture de session infructueuses depuis la dernière ouverture de session réussie.	Le soumissionnaire doit démontrer sa conformité en documentant sa capacité de répondre aux exigences, en utilisant des saisies d'écran ou des documents techniques ou d'utilisateur final pour compléter ses réponses.
M20	Le système proposé par le soumissionnaire doit afficher à l'utilisateur toutes les tentatives de connexion échouées depuis la dernière connexion réussie.	Le soumissionnaire doit démontrer sa conformité en documentant sa capacité de répondre aux exigences, en utilisant des saisies d'écran ou des documents techniques ou d'utilisateur final pour compléter ses réponses.
M21	<p>Le système proposé par le soumissionnaire doit permettre d'indiquer clairement sur tout écran d'affichage, fichier, imprimé ou courriel qu'il contient des données correspondant aux niveaux de confidentialité suivants (voir le glossaire pour les définitions) :</p> <ol style="list-style-type: none"> 1. Non classifié 2. Protégé A 3. Protégé B <p>*consulter les définitions des niveaux de confidentialité dans le glossaire.</p>	Le soumissionnaire doit démontrer sa conformité en documentant sa capacité de répondre aux exigences, en utilisant des saisies d'écran ou des documents techniques ou d'utilisateur final pour compléter ses réponses.
M22	Le soumissionnaire doit inclure dans sa soumission l'entente sur les niveaux de service publiée pour le système proposé. Les engagements de niveau de service inclus doivent fournir à EDSC des services de garantie, de maintenance et de soutien. Les services de soutien peuvent être fournis par téléphone, par courriel, par messagerie mobile ou par des outils Web, selon le cas.	Le soumissionnaire doit démontrer sa conformité en documentant sa capacité de répondre aux exigences, en utilisant des saisies d'écran ou des documents techniques ou d'utilisateur final pour compléter ses réponses.

ID	Exigence	Justification
M23	Le soutien du soumissionnaire doit permettre aux utilisateurs de signaler et de suivre les problèmes, en ligne ou par téléphone.	Le soumissionnaire doit démontrer sa conformité en documentant sa capacité de répondre aux exigences, en utilisant des saisies d'écran ou des documents techniques ou d'utilisateur final pour compléter ses réponses.
M24	Le soumissionnaire doit fournir la documentation qui décrit ses processus pour le système proposé : 1. Gestion de la configuration; 2. Gestion et contrôle du changement (p. ex., comme ITIL, Information Technology Infrastructure Library); 3. Gestion des services.	Le soumissionnaire doit démontrer sa conformité en documentant sa capacité de répondre aux exigences, en utilisant des saisies d'écran ou des documents techniques ou d'utilisateur final pour compléter ses réponses.
M25	Le soumissionnaire doit s'assurer que toutes les données du SACAGU seront accessibles au Canada, en format CSV, y compris le fichier de métadonnées, aux fins de rapatriement au Canada, dans les trois (3) mois suivant l'annulation de l'accès au système.	Le soumissionnaire doit démontrer sa conformité en documentant sa capacité de répondre aux exigences, en utilisant des saisies d'écran ou des documents techniques ou d'utilisateur final pour compléter ses réponses.
M26	Le soumissionnaire doit s'assurer que, sur demande du Canada, dans les cinq jours ouvrables, l'extrait de données du SACAGU sera disponible au Canada, en format CSV, y compris le fichier de métadonnées, aux fins de rapatriement au Canada.	Le soumissionnaire doit démontrer sa conformité en documentant sa capacité de répondre aux exigences, en utilisant des saisies d'écran ou des documents techniques ou d'utilisateur final pour compléter ses réponses.
M27	Le soumissionnaire doit fournir des services de soutien technique aux administrateurs du SACAGU par téléphone, courriel, messagerie mobile ou outils Web, selon le cas.	Le soumissionnaire doit démontrer sa conformité en documentant sa capacité de satisfaire aux exigences, en utilisant des saisies d'écran ou des documents techniques ou d'autres documents appropriés pour compléter sa réponse.

ID	Exigence	Justification
M28	La solution disponible sur le marché du soumissionnaire doit avoir la capacité, et le soumissionnaire doit être disposé, à la demande du Canada, à l'intégrer aux solutions demandées du marché pertinent ou aux systèmes sur place du Canada (p. ex., Microsoft Active Directory).	Le soumissionnaire doit démontrer sa conformité en documentant sa capacité de répondre aux exigences, en utilisant des saisies d'écran ou des documents techniques ou d'utilisateur final pour compléter ses réponses.

7.2. Exigences cotées

Ce qui suit s'applique à toutes les exigences cotées : Dans leur réponse, les soumissionnaires doivent démontrer leur conformité en fournissant la documentation décrivant leur capacité de répondre à l'exigence. Le soumissionnaire peut fournir des captures d'écran et des documents techniques ou d'utilisateur pour compléter sa réponse.

7.2.1. Exigences fonctionnelles - Cotées

Les exigences de cette section sont regroupées selon les principales fonctionnalités requises dans le SACAGU.

7.2.1.1 Gestion de la continuité des activités

ID	Exigence	Critères de notation	Justification
R1	Le système proposé par le soumissionnaire doit permettre aux utilisateurs d'EDSC de créer et de gérer les types suivants de documents de gestion des urgences (GU) : <ol style="list-style-type: none"> 1. Analyse des répercussions sur les activités 2. Plans de continuité des opérations 3. Plans d'urgence des immeubles 4. Plans de contingence 5. Plans de continuité des TI (p. ex. plan de reprise après sinistre) 6. Liste des applications essentielles 7. Listes de personnes-ressources 	Chacun des éléments énumérés vaut 2 points, pour un total de 32 points.	Le soumissionnaire doit démontrer sa conformité en documentant sa capacité de répondre aux exigences, en utilisant des saisies d'écran ou des documents techniques ou d'utilisateur final pour compléter ses réponses.

ID	Exigence	Critères de notation	Justification
	<ul style="list-style-type: none"> 8. Évaluation de la vulnérabilité ou des menaces et des risques de l'immeuble 9. Liste de vérification des inspections d'étages 10. Rapports de situation 11. Plans d'action 12. Calendrier des activités de GU 13. Rapports après action (RAA) 14. Questionnaires 15. Rapports de conformité, p. ex., achèvement du plan de GU, conformité du personnel de secours de l'immeuble (par étage, par immeuble) 16. Listes de contrôle 		
R2	<p>Le système proposé par le soumissionnaire devrait être en mesure d'aider les utilisateurs d'EDSC à gérer les composantes suivantes du programme Gestion de la continuité des activités :</p> <ul style="list-style-type: none"> 1. Cycles d'examen de la documentation 2. Évaluation des risques 3. Analyse des répercussions sur les activités 4. Plans d'intervention en cas d'incident 5. Plans de continuité des opérations 6. Plans de communication d'urgence 7. Documents de sensibilisation et de formation 8. Politiques et procédures 9. Plans de continuité des TI 	Chacun des éléments énumérés vaut 3 points, pour un total de 27 points.	Le soumissionnaire doit démontrer sa conformité en documentant sa capacité de répondre aux exigences, en utilisant des saisies d'écran ou des documents techniques ou d'utilisateur final pour compléter ses réponses.

ID	Exigence	Critères de notation	Justification
R3	<p>Le système proposé par le soumissionnaire doit comprendre une capacité d'analyse des répercussions sur les activités qui comprend la capacité d'évaluer les types d'incidence suivants :</p> <ol style="list-style-type: none"> 1. Incidence sur la santé des Canadiens/du public 2. Incidence sur la sûreté des Canadiens/du public 3. Incidence sur la sécurité des Canadiens/du public 4. Incidence sur le bien-être économique des Canadiens/du public 5. Incidence sur la fonction du gouvernement ou de l'organisation 6. Incidence sur la confiance et la réputation du public dans le Ministère ou l'organisation 7. Incidence sur la conformité juridique et réglementaire sur le Ministère ou l'organisation <p>Voir l'Annexe B pour les définitions des types d'incidence énumérés.</p>	<p>Chacun des éléments énumérés vaut 4 points, pour un total de 28 points.</p>	<p>Le soumissionnaire doit démontrer sa conformité en documentant sa capacité de répondre aux exigences, en utilisant des saisies d'écran ou des documents techniques ou d'utilisateur final pour compléter ses réponses.</p>
R4	<p>Le système proposé par le soumissionnaire devrait (p. ex., en utilisant des modèles) permettre d'utiliser les ensembles de données existants pour faciliter la saisie de modèles personnalisables.</p>	<p>La convivialité de cette capacité est :</p> <ol style="list-style-type: none"> 1. Facile pour les utilisateurs finaux et les administrateurs du SACAGU – 30 points 2. Facile soit pour l'utilisateur final, soit pour l'administrateur du SACAGU – 15 points 3. Pas facile pour tout type d'utilisateur – 0 point 	<p>Le soumissionnaire doit démontrer sa conformité en documentant sa capacité de répondre aux exigences, en utilisant des saisies d'écran ou des documents techniques ou d'utilisateur final pour compléter ses réponses.</p>

ID	Exigence	Critères de notation	Justification
R5	<p>Le système proposé par le soumissionnaire doit permettre de créer des modèles (format, disposition et champs de données) pour chaque type de plan et de rapport de gestion des urgences (GU).</p> <p>Le système proposé devrait permettre à l'utilisateur :</p> <ol style="list-style-type: none"> 1. D'inclure les champs de données définis par EDSC, notamment : <ol style="list-style-type: none"> i. Données de documents électroniques créés précédemment ii. Données entrées manuellement par les utilisateurs d'EDSC iii. Données provenant d'ensembles de données publiques (p. ex., données des cartes de Google). iv. Toute donnée d'EDSC 2. De définir le format du document électronique connexe, notamment : <ol style="list-style-type: none"> i. Disposition (emplacement des champs) ii. En-têtes iii. Titre iv. Orientation des pages v. Tableaux vi. Figures 	Chacun des éléments énumérés vaut 2 points, pour un total de 20 points.	Le soumissionnaire doit démontrer sa conformité en documentant sa capacité de répondre aux exigences, en utilisant des saisies d'écran ou des documents techniques ou d'utilisateur final pour compléter ses réponses.
R6	<p>Le système proposé par le soumissionnaire devrait inclure un modèle de liste de personnes-ressources. Le modèle de liste de personnes-ressources doit être configurable pour permettre aux utilisateurs de saisir les données suivantes concernant la personne-ressource :</p>	Chacun des éléments énumérés vaut 1 point, pour un total de 10 points.	Le soumissionnaire doit démontrer sa conformité en documentant sa capacité de répondre aux exigences, en utilisant des saisies d'écran ou des documents techniques ou d'utilisateur final pour compléter ses réponses.

ID	Exigence	Critères de notation	Justification
	<ol style="list-style-type: none"> 1. Nom 2. Titre 3. Structure organisationnelle à laquelle il appartient 4. Téléphone(s) cellulaire(s)/BlackBerry cellulaire/Télécopieur 5. Téléphone à la maison 6. Courriel interne et externe 7. Compétences ou capacité particulières (p. ex., réanimation cardiorespiratoire [RCR], premiers soins, accès à un RPV, rôle au sein du personnel d'urgence de l'immeuble) 8. Travail à l'extérieur des locaux 9. Emplacement (p. ex., immeuble) 10. Champs personnalisés 		

7.2.1.2. Gestion de la continuité des activités

ID	Exigence	Critères de notation	Justification
R7	<p>Le modèle d'analyse des répercussions sur les activités (ARA) proposé par le soumissionnaire doit être configurable pour saisir les données suivantes :</p> <ol style="list-style-type: none">1. Fonctions et services opérationnels identifiés,2. Objectifs de temps de reprise (y compris les dépendances de la TI),3. Objectifs des points de reprise (y compris les dépendances en matière de TI),4. Temps d'arrêt maximal admissible5. Niveau de service normal6. Niveau de service minimal7. Répercussion des interruptions,8. Temps de fonctionnement essentiel et de pointe,9. Interdépendances en aval (p. ex., qui compte sur vous, interne par rapport à externe),10. Interdépendances en amont (p. ex., de qui dépendez-vous?)11. Dépendances de la technologie de l'information (p. ex., applications incluant types, systèmes, infrastructure)12. Infrastructure essentielle (p. ex., infrastructure de réseautage, stockage, centre de données).13. Exigences minimales en matière de ressources (p. ex., niveaux de dotation).	<p>Chacun des éléments énumérés vaut 1 point, pour un total de 13 points.</p>	<p>Le soumissionnaire doit démontrer sa conformité en documentant sa capacité de répondre aux exigences, en utilisant des saisies d'écran ou des documents techniques ou d'utilisateur final pour compléter ses réponses.</p>

R8	<p>Le modèle de plan de continuité des activités (PCA) proposé par le soumissionnaire doit être configurable pour saisir les données suivantes :</p> <ol style="list-style-type: none"> 1. Profil (description) 2. Plan de mise en œuvre du PCA 3. Liste de vérification pour la reprise 4. Stratégie de communication 5. Organigrammes pour l'équipe de gestion de crise 6. Fonctions ou services opérationnels essentiels et stratégies de reprise (notamment ODR, DIMA, ODR, interdépendances). 7. Fonctions ou services opérationnels non critiques 8. Multiples listes de personnes-ressources pour tout le personnel essentiel 9. Lieux de travail de remplacement (p. ex., sous-ministre, activités essentielles) 10. Structure organisationnelle configurable (p. ex., service, équipe d'évacuation d'urgence de l'immeuble) 11. Liste des personnes-ressources externes en cas d'urgence (p. ex., premiers intervenants). 12. Inventaire des équipements, biens et logiciels essentiels 13. Cartes et itinéraires pour les lieux des réunions d'urgence 14. Information locale et communautaire. 15. Journal des incidents et des interventions de l'équipe du PCA 16. Registre des documents du PCA 17. Documents essentiels (procédures opérationnelles normalisées – PON, procédures manuelles de rechange, dossiers papier). 	Chacun des éléments énumérés vaut 1 point, pour un total de 17 points.	Le soumissionnaire doit démontrer sa conformité en documentant sa capacité de répondre aux exigences, en utilisant des saisies d'écran ou des documents techniques ou d'utilisateur final pour compléter ses réponses.
----	--	--	--

ID	Exigence	Critères de notation	Justification
R9	Le système proposé par le soumissionnaire doit inclure la capacité d'élaborer des stratégies de reprise et leurs analyses coûts-avantages respectives.	<p>Le système proposé par le soumissionnaire :</p> <ol style="list-style-type: none"> 1. Appuie entièrement l'élaboration de stratégies de reprise fondées sur les données d'entrée, y compris l'analyse coûts-avantages – 10 points. 2. Appuie entièrement l'élaboration de stratégies de reprise fondées sur les données d'entrée, mais ne comprend pas l'analyse coûts-avantages connexe – 6 points. 3. Contient uniquement des champs de texte pour consigner les stratégies de reprise et les coûts connexes – 3 points. 4. N'appuie ni l'élaboration de stratégies de reprise ni l'analyse coûts-avantages – 0 point 	Le soumissionnaire doit démontrer sa conformité en documentant sa capacité de répondre aux exigences, en utilisant des saisies d'écran ou des documents techniques ou d'utilisateur final pour compléter ses réponses.
R10	<p>Le système proposé par le soumissionnaire doit satisfaire aux principales normes de gestion de la continuité des activités (GCA) suivantes :</p> <ol style="list-style-type: none"> 1. ISO 22301 (Gestion de la continuité des activités) 2. ISO 27031 (reprise après sinistre des TI) 3. ISO 31000 Techniques de gestion du risque 	<p>Le système proposé par le soumissionnaire :</p> <ol style="list-style-type: none"> 1. Satisfait à toutes les normes énumérées – 10 points 2. Satisfait à deux des normes énumérées – 6 points 3. Satisfait à l'une des normes énumérées – 3 points 4. Ne satisfait à aucune des normes énumérées – 0 point 	<p>Le soumissionnaire doit démontrer sa conformité en fournissant les certifications énumérées.</p> <p>Si le soumissionnaire est en voie d'obtenir ces certifications, il doit en fournir la preuve, à l'aide d'autres documents pertinents ou de saisies d'écran démontrant le fondement.</p>

7.2.1.3.

Gestion

des

urgences

ID	Exigence	Critères de notation	Justification
R11	<p>Le plan d'urgence et d'évacuation de l'immeuble proposé par le soumissionnaire doit être configurable afin de permettre la saisie des données suivantes :</p> <ol style="list-style-type: none"> 1. Coordonnées d'urgence (internes et externes). 2. Liste configurable de l'équipement et des systèmes et équipements d'urgence de l'immeuble. 3. Renseignements sur l'occupation (p. ex., population d'occupants, % d'occupation locataire principal/locataire secondaire) 4. Plans d'étage et dessins architecturaux 5. Renseignements sur l'immeuble (p. ex., ascenseurs, heures normales, alertes, hauteur et taille de l'immeuble) 6. Procédures d'urgence 7. Rôles et responsabilités du personnel d'urgence de l'immeuble 8. Personne-ressource 9. Registre des activités du personnel d'urgence de l'immeuble 10. Carte des lieux de rassemblement en cas d'urgence 11. Pièces jointes diverses (p. ex., registre des activités du personnel d'urgence de l'immeuble, organigrammes, copie du pompiers) 12. Liste de vérification des vulnérabilités de l'immeuble 13. Partage de locaux (p. ex., autres ministères du Canada, organismes privés, etc.) 14. Liste du personnel d'urgence de l'immeuble par étage 	Chacun des éléments énumérés vaut 2 points, pour un total de 28 points.	Le soumissionnaire doit démontrer sa conformité en documentant sa capacité de répondre aux exigences, en utilisant des saisies d'écran ou des documents techniques ou d'utilisateur final pour compléter ses réponses.
R12	Le système proposé par le soumissionnaire devrait permettre aux utilisateurs d'EDSC de	Chacun des éléments énumérés vaut 4 points, pour un total de 20 points.	Le soumissionnaire doit démontrer sa conformité en documentant sa capacité

ID	Exigence	Critères de notation	Justification
	<p>créer et de gérer des listes de vérification. Ces listes de vérification doivent contenir des données sur les éléments suivants :</p> <ol style="list-style-type: none"> 1. Dangers en milieu de travail 2. Équipement d'intervention d'urgence 3. Équipement de santé et de sécurité 4. Équipes et personnel d'urgence 5. Formation 		de répondre aux exigences, en utilisant des saisies d'écran ou des documents techniques ou d'utilisateur final pour compléter ses réponses.

7.2.1.4. Planification de la continuité de la TI

ID	Exigence	Critères de notation	Justification
R13	<p>Le modèle du système proposé par le soumissionnaire pour le plan de continuité de la TI (ou plan de reprise après sinistre) doit être configurable pour saisir les données suivantes :</p> <ol style="list-style-type: none"> 1. Buts et objectifs 2. Portée 3. Hypothèses et limites 4. Définitions 5. Rôles et responsabilités (p. ex., listes de personnes-ressources et équipes) 6. Aperçu du système – Nom du système, acronyme, ID 7. Aperçu de l'infrastructure de continuité de la TI (p. ex., diagrammes, listes, etc.) 8. Ententes sur les niveaux de service 9. Capacité d'évaluation des incidences (capacité d'établir des liens avec les services essentiels) 10. Procédure d'activation du plan (p. ex., mention des intervenants qui peuvent activer le plan) 	Chacun des éléments énumérés vaut 1 point, pour un total de 24 points.	Le soumissionnaire doit démontrer sa conformité en documentant sa capacité de répondre aux exigences, en utilisant des saisies d'écran ou des documents techniques ou d'utilisateur final pour compléter ses réponses.

ID	Exigence	Critères de notation	Justification
	<ul style="list-style-type: none"> 11. Signalement de l'incident 12. Procédures de rétablissement 13. Validation du rétablissement 14. Procédures de traitement de secours 15. Processus de communication 16. Procédure de signalement aux échelons supérieurs 17. Considérations relatives à la sécurité de la TI 18. Piste de vérification des modifications apportées aux documents 19. Essais et exercices 20. Capacité d'exploiter les métadonnées du système, y compris les données de l'analyse des incidences sur les activités, les plans de continuité des activités, etc. 21. Objectif de délai de reprise des systèmes de TI 22. Objectif de point de reprise des systèmes de TI 23. Temps d'arrêt maximal admissible – pour les services opérationnels essentiels 24. Personne-ressource du programme de continuité de la TI d'EDSC 		

7.2.1.5. Gestion de crise

ID	Exigence	Critères de notation	Justification
R14	<p>Le système proposé par le soumissionnaire devrait être en mesure d'aider les utilisateurs d'EDSC à gérer les urgences et les incidents de TI et à en rendre compte au moyen des fonctions suivantes :</p> <ol style="list-style-type: none"> 1. Création de l'incident 2. Notification de l'incident 3. Transmission des incidents aux paliers supérieurs 4. Gestion de l'incident 5. Fermeture de l'incident 6. Rapports sur l'incident 7. Création d'une liste de contrôle des mesures 8. Capacité de tirer parti d'autres sources de données d'EDSC, comme les plans de gestion des urgences. 	Chacun des éléments énumérés vaut 4 points, pour un total de 32 points.	Le soumissionnaire doit démontrer sa conformité en documentant sa capacité de répondre aux exigences, en utilisant des saisies d'écran ou des documents techniques ou d'utilisateur final pour compléter ses réponses.
R15	<p>Le modèle de plan d'action en cas d'incident du système proposé par le soumissionnaire doit être configurable pour saisir les données suivantes :</p> <ol style="list-style-type: none"> 1. Type d'urgence 2. Heure du signalement 3. Objectif(s) 4. Stratégies pour l'atteinte des objectifs 5. Date/heure d'achèvement estimée 6. État au moment du signalement 	Chacun des éléments énumérés vaut 5 points, pour un total de 30 points.	Le soumissionnaire doit démontrer sa conformité en documentant sa capacité de répondre aux exigences, en utilisant des saisies d'écran ou des documents techniques ou d'utilisateur final pour compléter ses réponses.
R16	<p>Le système proposé par le soumissionnaire doit fournir une fonction de notification de masse en cas d'urgence, intégrée ou externe, capable de transmettre des messages d'urgence de masse ciblés par quatre canaux :</p> <ol style="list-style-type: none"> 1. Courriel; 	<p>Le système proposé par le soumissionnaire prend en charge un système d'avertissement de masse en cas d'urgence :</p> <ol style="list-style-type: none"> 1. Entièrement, par l'entremise des quatre canaux énumérés et 	Le soumissionnaire doit démontrer sa conformité en documentant sa capacité de répondre aux exigences, en utilisant des saisies d'écran ou des documents techniques ou d'utilisateur final pour compléter ses réponses.

ID	Exigence	Critères de notation	Justification
	2. Messagerie instantanée; 3. Appareil mobile; 4. Téléphone fixe.	<p>comprend des moyens d'identifier la transmission du message et la confirmation de réception. - 20 points</p> <p>2. Par l'entremise d'au moins deux des canaux énumérés et comprend des moyens d'identifier la transmission du message et la confirmation de réception. - 15 points</p> <p>3. Par l'un des canaux énumérés et comprend des moyens d'identifier la transmission du message et la confirmation de réception; OU</p> <p>par plus d'un des canaux énumérés, mais ne comprend pas de moyens d'identifier la livraison du message et la confirmation de la réception. - 10 points</p> <p>4. Par l'un des canaux énumérés, mais ne comprend pas de moyens d'identifier la livraison du message et la confirmation de réception. – 5 points</p> <p>5. Impossible de prendre en charge un système d'avertissement de masse en cas d'urgence – 0 point</p>	
R17	Le système proposé par le soumissionnaire doit permettre aux utilisateurs d'EDSC d'envoyer des notifications (p. ex., préapprouvées ou spéciales) aux utilisateurs d'EDSC par l'entremise des moyens suivants :	Chacun des éléments énumérés vaut 3 points, pour un total de 12 points.	Le soumissionnaire doit démontrer sa conformité en documentant sa capacité de répondre aux exigences, en utilisant des saisies d'écran ou des documents

ID	Exigence	Critères de notation	Justification
	<ol style="list-style-type: none"> 1. Courriel préapprouvé 2. Courriel spécial 3. Texte préapprouvé 4. Texte spécial 		techniques ou d'utilisateur final pour compléter ses réponses.
R18	<p>Le système proposé par le soumissionnaire devrait être en mesure de mettre à jour les champs de données d'EDSC contenus dans les notifications préapprouvées dans l'ensemble de données pertinent le plus récent avant d'envoyer des notifications préapprouvées. Ces champs permettent de saisir les données suivantes :</p> <ol style="list-style-type: none"> 1. Date 2. Heure 3. Emplacement (c.-à-d. étage(s), immeuble, région) 4. Nom et type d'urgence 5. Mesures d'urgence 	Chacun des éléments énumérés vaut 2 points, pour un total de 10 points.	Le soumissionnaire doit démontrer sa conformité en documentant sa capacité de répondre aux exigences, en utilisant des saisies d'écran ou des documents techniques ou d'utilisateur final pour compléter ses réponses.

7.2.1.6.

Exercices

ID	Exigence	Critères de notation	Justification
R19	<p>Le système proposé par le soumissionnaire doit permettre aux utilisateurs d'EDSC de planifier les activités de gestion des urgences (GU) suivantes :</p> <ol style="list-style-type: none"> 1. Exercices de gestion de la continuité des activités 2. Exercices de GU 3. Exercices de continuité des activités de la TI 	Chacun des éléments énumérés vaut 5 points, pour un total de 30 points.	Le soumissionnaire doit démontrer sa conformité en documentant sa capacité de répondre aux exigences, en utilisant des saisies d'écran ou des documents techniques ou d'utilisateur final pour compléter ses réponses.

ID	Exigence	Critères de notation	Justification
	4. Cycles de création et d'examen des documents électroniques 5. Formation du personnel d'urgence des immeubles 6. Activités de sensibilisation à la GU		
R20	<p>Le système proposé par le soumissionnaire, tout en planifiant les activités de gestion des urgences (GU), devrait permettre de saisir les données suivantes :</p> <ol style="list-style-type: none"> 1. Direction générale/région 2. Type d'activité de GU 3. Jour, mois et année de l'activité de GU 4. Nom du responsable de l'activité de GU 5. Titre de l'activité de GU 6. Objectif de l'activité de GU 	Chacun des éléments énumérés vaut 2 points, pour un total de 12 points.	Le soumissionnaire doit démontrer sa conformité en documentant sa capacité de répondre aux exigences, en utilisant des saisies d'écran ou des documents techniques ou d'utilisateur final pour compléter ses réponses.
R21	<p>Le système proposé par le soumissionnaire doit permettre de gérer et d'exécuter les types d'exercices de gestion des urgences suivants et d'en rendre compte :</p> <ol style="list-style-type: none"> 1. Exercices axés sur la discussion (p. ex., revue générale) 2. Exercices pratiques (p. ex., confinement, évacuation, intrus actif) 3. Exercices de simulation (p. ex., opérationnels et fonctionnels) 4. Exercices à grande échelle 5. Continuité de la TI et reprise après sinistre 	Chacun des éléments énumérés vaut 4 points, pour un total de 20 points.	Le soumissionnaire doit démontrer sa conformité en documentant sa capacité de répondre aux exigences, en utilisant des saisies d'écran ou des documents techniques ou d'utilisateur final pour compléter ses réponses.

ID	Exigence	Critères de notation	Justification
R22	<p>Le système proposé par le soumissionnaire doit permettre de créer et/ou de personnaliser des modèles, par exemple pour les types suivants de documentation d'exercice :</p> <p>Ordres du jour</p> <p>Liste chronologique des événements</p> <p>Fiche d'intrants</p> <p>Manuel de l'animateur</p> <p>Manuel du contrôleur</p> <p>Manuel de l'évaluateur</p> <p>Manuel des joueurs</p> <p>Guide de l'observateur</p> <p>Formulaire d'évaluation du participant</p> <p>Formulaire d'évaluation de l'observateur</p> <p>Formulaire d'évaluation de l'exercice</p> <p>Rapport après action</p> <p>Plan d'action de la gestion</p> <p>Plan de communication</p> <p>Plan de l'exercice</p>	<p>Chacun des éléments énumérés vaut 1 point, pour un total de 15 points.</p> <p>Cette capacité du système proposé par le soumissionnaire est :</p> <ol style="list-style-type: none"> 1. Complète et facile, tant pour l'utilisateur final que l'administrateur du SACAGU – 15 points 2. Complet et facile, soit pour l'utilisateur final ou l'administrateur du SACAGU – 10 points 3. Partielle, facile tant pour l'utilisateur final que pour l'administrateur du SACAGU – 5 points 4. Partielle, facile pour l'utilisateur final ou l'administrateur du SACAGU – 0 point 	<p>Le soumissionnaire doit démontrer sa conformité en documentant sa capacité de répondre aux exigences, en utilisant des saisies d'écran ou des documents techniques ou d'utilisateur final pour compléter ses réponses.</p>
R23	<p>Le système proposé par le soumissionnaire doit permettre de :</p> <ol style="list-style-type: none"> 1. Planifier de la formation et de la sensibilisation; 2. Surveiller et suivre l'exécution des activités énumérées ci-dessous à l'aide d'un produit graphique; 3. Rendre compte des progrès des activités énumérées ci-dessous; 4. Signaler automatiquement les activités non conformes ou en retard. <p>pour chacun des types d'activités suivants :</p>	<p>Pour les activités énumérées de formation et de sensibilisation des employés en cas d'urgence et les exercices d'urgence dans les immeubles, le système proposé par le soumissionnaire :</p> <ol style="list-style-type: none"> 1. Comprend les quatre fonctionnalités numérotées qui couvrent les six activités énumérées – 10 points 2. Ne comporte que les fonctionnalités 1, 2 et 3 pour 	<p>Le soumissionnaire doit démontrer sa conformité en documentant sa capacité de répondre aux exigences, en utilisant des saisies d'écran ou des documents techniques ou d'utilisateur final pour compléter ses réponses.</p>

ID	Exigence	Critères de notation	Justification
	<p>1. Activités de formation et de sensibilisation des employés pour les situations d'urgence, notamment :</p> <ul style="list-style-type: none"> i. Formation sur le SACAGU, ii. Séances de sensibilisation aux intrus armés, iii. Intervention de cybersécurité iv. Continuité de la TI. <p>2. Exercices d'urgence dans l'immeuble, notamment :</p> <ul style="list-style-type: none"> i. Exercices d'incendie, ii. Exercices de confinement. 	<p>couvrir les six activités énumérées – 8 points</p> <p>3. Ne comporte que les fonctionnalités 1, 2 et 3, mais la fonctionnalité 2 ne peut surveiller que deux à cinq des activités énumérées – 6 points</p> <p>4. Ne comporte que les fonctionnalités 1, 2 et 3, mais la fonctionnalité 1 peut permettre de planifier la formation et la sensibilisation des employés ou les exercices d'urgence de l'immeuble et la fonctionnalité 2 ne peut surveiller que deux à cinq des activités énumérées – 4 points</p> <p>5. Ne comporte que la fonctionnalité 2, qui ne peut surveiller que deux à cinq des activités énumérées – 2 points</p> <p>6. Ne comporte aucune fonctionnalité indiquée pour aucune des activités indiquées – 0 point</p>	

7.2.1.7. Gestion des données

ID	Exigence	Critères de notation	Justification
R24	<p>Le système proposé par le soumissionnaire doit permettre de créer des relations entre les données ou les renseignements d'EDSC (documents et rapports électroniques) contenus dans le SACAGU, notamment :</p> <ol style="list-style-type: none"> 1. Lieux (p. ex., étage, nom de l'immeuble, type de bâtiment, région géographique définie, ville, province, région géographique définie par EDSC) 2. Services essentiels 3. Dépendances de la TI 4. Responsables des plans de gestion des urgences ou de continuité des activités 	Chacun des éléments énumérés vaut 8 points, pour un total de 32 points.	Le soumissionnaire doit démontrer sa conformité en documentant sa capacité de répondre aux exigences, en utilisant des saisies d'écran ou des documents techniques ou d'utilisateur final pour compléter ses réponses.
R25	<p>Le système proposé par le soumissionnaire doit permettre aux administrateurs du SACAGU de :</p> <ol style="list-style-type: none"> 1. Modifier et ajouter des étiquettes de champ sur l'interface utilisateur et les modèles, sans l'aide de l'entrepreneur (fournisseur de couches SaaS); 2. Reproduire les nouvelles étiquettes dans tous les documents électroniques applicables. 	<p>Le système proposé par le soumissionnaire comporte :</p> <ol style="list-style-type: none"> 1. Les deux fonctionnalités indiquées – 10 points 2. La première fonctionnalité indiquée seulement – 5 points 3. Aucune des fonctionnalités indiquées – 0 point 	Le soumissionnaire doit démontrer sa conformité en documentant sa capacité de répondre aux exigences, en utilisant des saisies d'écran ou des documents techniques ou d'utilisateur final pour compléter ses réponses.
R26	<p>Le système proposé par le soumissionnaire devrait permettre de signaler la conservation de :</p> <ol style="list-style-type: none"> 1. Documents et rapports électroniques; 2. Métadonnées connexes; 3. Registres de vérification connexes. 	<p>Le système proposé par le soumissionnaire comporte :</p> <ol style="list-style-type: none"> 1. La fonctionnalité complète permettant de signaler les documents électroniques, les métadonnées et les registres de 	Le soumissionnaire doit démontrer sa conformité en documentant sa capacité de répondre aux exigences, en utilisant des saisies d'écran ou des documents techniques ou d'utilisateur final pour compléter ses réponses.

ID	Exigence	Critères de notation	Justification
R27	<p>Le système proposé par le soumissionnaire doit fournir une capacité de saisie et de production de rapports liés aux vérifications qui comprend une piste de vérification pour :</p> <ol style="list-style-type: none"> 1. Les actions de l'utilisateur 2. Les activités administratives (p. ex., création et modification de comptes d'utilisateur) 3. Les autorisations d'accès de l'utilisateur 4. Les changements de configuration apportés au SACAGU. 5. Les modifications du contenu d'EDSC (y compris les données et les documents électroniques d'EDSC) 6. La création de documents électroniques (p. ex., contrôle des versions) 	<p>vérification à des fins de conservation – 10 points</p> <ol style="list-style-type: none"> 2. La fonctionnalité permettant de signaler deux des trois types de fichiers (documents électroniques, métadonnées ou registres de vérification) aux fins de conservation – 6 points 3. La Fonctionnalité permettant de signaler l'un des trois types de fichiers (documents électroniques, métadonnées ou registres de vérification) aux fins de conservation – 3 points 4. Aucune fonctionnalité permettant de signaler les documents électroniques, les métadonnées et les registres de vérification à des fins de conservation – 0 point <p>Chacun des éléments énumérés vaut 3 points, pour un total de 21 points.</p>	<p>Le soumissionnaire doit démontrer sa conformité en documentant sa capacité de répondre aux exigences, en utilisant des saisies d'écran ou des documents techniques ou d'utilisateur final pour compléter ses réponses.</p>

ID	Exigence	Critères de notation	Justification
	7. L'accès, la modification et la suppression non autorisés des données d'EDSC		
R28	Le système proposé par le soumissionnaire doit permettre aux utilisateurs d'EDSC de visualiser et de suivre les versions historiques (p. ex., le contrôle des versions) des documents électroniques, y compris les dix versions les plus récentes.	<p>Le système proposé par le soumissionnaire :</p> <ol style="list-style-type: none"> 1. Peut afficher un nombre défini par l'administrateur de versions historiques des documents, au moins les dix précédentes - 10 points 2. Peut afficher un nombre fixe de versions historiques de documents, au moins les dix précédentes - 8 points 3. Peut afficher un nombre fixe ou défini par l'administrateur de versions historiques des documents, au moins les cinq précédentes - 6 points 4. Peut afficher un nombre fixe ou défini par l'administrateur de versions historiques de documents, au moins les trois précédentes - 3 points 	Le soumissionnaire doit démontrer sa conformité en documentant sa capacité de répondre aux exigences, en utilisant des saisies d'écran ou des documents techniques ou d'utilisateur final pour compléter ses réponses.

ID	Exigence	Critères de notation	Justification
R29	Le système proposé par le soumissionnaire devrait permettre aux administrateurs d'EDSC de configurer le nombre d'actions antérieures que les utilisateurs d'EDSC peuvent annuler.	<p>5. Ne peut afficher jusqu'à dix versions historiques de documents – 0 point</p> <p>Le système proposé par le soumissionnaire :</p> <ol style="list-style-type: none"> 1. Offre la fonctionnalité permettant aux administrateurs d'EDSC de configurer le nombre d'actions antérieures que les utilisateurs d'EDSC peuvent annuler – 10 points 2. N'offre pas aux administrateurs d'EDSC la fonctionnalité permettant de configurer le nombre d'actions antérieures que les utilisateurs d'EDSC peuvent annuler – 0 point 	Le soumissionnaire doit démontrer sa conformité en documentant sa capacité de répondre aux exigences, en utilisant des saisies d'écran ou des documents techniques ou d'utilisateur final pour compléter ses réponses.
R30	Le système proposé par le soumissionnaire devrait permettre de sélectionner des données à partir de listes prédéterminées, notamment : <ol style="list-style-type: none"> 1. Menus déroulants 2. Listes de sélection 3. Recherche 	Chacun des éléments énumérés vaut 6 points, pour un total de 18 points.	Le soumissionnaire doit démontrer sa conformité en documentant sa capacité de répondre aux exigences, en utilisant des saisies d'écran ou des documents techniques ou d'utilisateur final pour compléter ses réponses.
R31	Le système proposé par le soumissionnaire devrait permettre de migrer les données existantes. Le Canada fournira les données au soumissionnaire en format CSV.	<p>Le système proposé par le soumissionnaire :</p> <ol style="list-style-type: none"> 1. Peut migrer toutes les données existantes prévues, lorsque la fonctionnalité est suffisamment importante pour que l'administrateur du SACAGU puisse la réaliser sans l'aide de l'entrepreneur – 20 points 	Le soumissionnaire doit démontrer sa conformité en documentant sa capacité de répondre aux exigences, en utilisant des saisies d'écran ou des documents techniques ou d'utilisateur final pour compléter ses réponses.

ID	Exigence	Critères de notation	Justification
		<p>2. Peut migrer toutes les données existantes prévues, mais la fonctionnalité est telle qu'elle ne peut être réalisée qu'avec l'aide de la ressource professionnelle de l'entrepreneur – 10 points</p> <p>3. Ne peut migrer aucune donnée existante – 0 point</p>	

7.2.1.8. Flux de travail

ID	Exigence	Critères de notation	Justification
R32	<p>Le système proposé par le soumissionnaire devrait identifier automatiquement (p. ex., signaler) l'état des flux de travaux et des tâches à l'aide d'identificateurs uniques :</p> <ol style="list-style-type: none"> 1. En retard 2. Terminé 3. Incomplet 4. Approuvé 5. Soumis 6. Prévu 7. En révision 8. En cours 	Chacun des éléments énumérés vaut 1 point, pour un total de 8 points.	Le soumissionnaire doit démontrer sa conformité en documentant sa capacité de répondre aux exigences, en utilisant des saisies d'écran ou des documents techniques ou d'utilisateur final pour compléter ses réponses.

ID	Exigence	Critères de notation	Justification
R33	<p>Le système proposé par le soumissionnaire devrait permettre de consulter et de produire des rapports sur les activités du flux de travail. Ces flux de travail et rapports incluraient les renseignements suivants :</p> <ol style="list-style-type: none"> 1. fréquence de l'utilisation; 2. % de plans de gestion des urgences (GU) ou de continuité des activités (CA) approuvés; 3. % de plans de GU et/ou de CA en cours (création/examen); 4. % de plans de GU ou de CA manquants; 5. % d'exercices de GU et/ou de CA prévus; 6. % d'exercices de GU et/ou de CA exécutés dans les délais prévus. 	Chacun des éléments énumérés vaut 2 points, pour un total de 12 points.	Le soumissionnaire doit démontrer sa conformité en documentant sa capacité de répondre aux exigences, en utilisant des saisies d'écran ou des documents techniques ou d'utilisateur final pour compléter ses réponses.
R34	<p>Le système proposé par le soumissionnaire doit permettre aux utilisateurs du SACAGU de recevoir des notifications automatiques des flux de travail, des tâches et des mesures attribués, ce qui comprendrait l'information suivante :</p> <ol style="list-style-type: none"> 1. Tâches assignées; 2. Tâches réassignées; 3. Tâches achevées; 4. Tâches acceptées; 5. Tâches refusées. 	Chacun des éléments énumérés vaut 2 points, pour un total de 10 points.	Le soumissionnaire doit démontrer sa conformité en documentant sa capacité de répondre aux exigences, en utilisant des saisies d'écran ou des documents techniques ou d'utilisateur final pour compléter ses réponses.
R35	<p>Le système proposé par le soumissionnaire devrait permettre aux utilisateurs du SACAGU d'identifier manuellement (c.-à-d. de signaler) les documents électroniques, les rapports et les données d'EDSC pour les :</p>	Chacun des éléments énumérés vaut 3 points, pour un total de 9 points.	Le soumissionnaire doit démontrer sa conformité en documentant sa capacité de répondre aux exigences, en utilisant des saisies d'écran ou des documents techniques ou d'utilisateur final pour compléter ses réponses.

ID	Exigence	Critères de notation	Justification
	1. Mises à jour; 2. Révisions; 3. Demandes de renseignements.		

7.2.1.9. Gestion de comptes

ID	Exigence	Critères de notation	Justification
R36	<p>Le système proposé par le soumissionnaire doit permettre aux administrateurs du SACAGU ou aux coordonnateurs du SACAGU de créer des comptes d'utilisateur ayant les attributs suivants :</p> <ol style="list-style-type: none">1. Nom2. Titre du poste3. Fonction de gestion des urgences4. Région / direction générale5. Secteur d'activités6. Direction7. Division8. Rôle du SACAGU (se référer aux définitions sous Rôles du SACAGU, à la page 4)9. Date d'expiration de l'accès au SACAGU10. Coordonnées :<ol style="list-style-type: none">i. Courriel;ii. Numéros de téléphone.11. Lieu de travail :<ol style="list-style-type: none">i. Ville;ii. Province;iii. Numéro civique et nom de la rue;iv. Étage;v. Numéro du local ou du bureau.	Chacun des éléments énumérés vaut 1 point, pour un total de 11 points.	Le soumissionnaire doit démontrer sa conformité en documentant sa capacité de répondre aux exigences, en utilisant des saisies d'écran ou des documents techniques ou d'utilisateur final pour compléter ses réponses.

ID	Exigence	Critères de notation	Justification
R37	<p>Le système proposé par le soumissionnaire doit permettre aux administrateurs du SACAGU d'attribuer les privilèges suivants de compte d'utilisateur, en fonction des rôles : Administrateur du SACAGU, coordonnateur du SACAGU, contributeur au SACAGU, examinateur du SACAGU :</p> <ol style="list-style-type: none"> 1. Accès en lecture 2. Contribuer (p. ex., modifier et signaler les documents électroniques) 3. Créer un document électronique 4. Soumettre un document électronique 5. Approuver un document électronique 6. Accorder ou retirer des privilèges 7. Modifier les propriétés des documents électroniques 8. Attribuer les tâches suivantes aux utilisateurs : <ol style="list-style-type: none"> i. Remplir un document électronique ii. Mettre à jour un document électronique iii. Réviser un document électronique iv. Approuver un document électronique v. Ajouter des renseignements supplémentaires aux documents électroniques 9. Modifier une tâche 10. Supprimer une tâche 11. Téléverser/télécharger les données/documents électroniques d'EDSC 	Chacun des éléments énumérés vaut 2 points, pour un total de 22 points.	Le soumissionnaire doit démontrer sa conformité en documentant sa capacité de répondre aux exigences, en utilisant des saisies d'écran ou des documents techniques ou d'utilisateur final pour compléter ses réponses.

ID	Exigence	Critères de notation	Justification
R38	Le système proposé par le soumissionnaire doit permettre aux administrateurs du SACAGU de retirer les privilèges des comptes d'utilisateur des utilisateurs du SACAGU, sans qu'il soit nécessaire de retirer les privilèges du profil d'un fichier individuel.	<p>Le système proposé par le soumissionnaire :</p> <ol style="list-style-type: none"> 1. Offre aux administrateurs une fonctionnalité permettant de retirer des comptes d'utilisateur sans avoir à retirer les privilèges dans les fichiers individuels – 10 points 2. Offre à l'entrepreneur une fonctionnalité permettant de retirer les comptes d'utilisateur sans avoir à retirer les privilèges dans les fichiers individuels – 5 points 3. N'offre aucune fonctionnalité permettant de retirer les comptes d'utilisateur sans avoir à retirer les privilèges dans les fichiers individuels – 0 point 	Le soumissionnaire doit démontrer sa conformité en documentant sa capacité de répondre aux exigences, en utilisant des saisies d'écran ou des documents techniques ou d'utilisateur final pour compléter ses réponses.

ID	Exigence	Critères de notation	Justification
R39	Le système proposé par le soumissionnaire devrait permettre aux administrateurs du SACAGU de restreindre l'accès aux données, aux documents électroniques et aux rapports d'EDSC en fonction de critères prédéfinis (p. ex., groupes – division, direction, direction générale/région, immeuble).	<p>Le système proposé par le soumissionnaire :</p> <ol style="list-style-type: none"> 1. Peut restreindre l'accès en fonction de tous les critères prédéfinis pour l'organisation et l'immeuble – 20 points 2. Peut restreindre l'accès en fonction soit de l'immeuble ou de critères organisationnels - 10 points 3. Ne peut restreindre l'accès en fonction de critères prédéfinis – 0 point 	Le soumissionnaire doit démontrer sa conformité en documentant sa capacité de répondre aux exigences, en utilisant des saisies d'écran ou des documents techniques ou d'utilisateur final pour compléter ses réponses.
R40	Le système proposé par le soumissionnaire devrait permettre la gestion des comptes d'utilisateur, y compris la surveillance et la production de rapports à cet égard.	<p>Le système proposé par le soumissionnaire :</p> <ol style="list-style-type: none"> 1. Possède des capacités de gestion des comptes d'utilisateur, ce qui comprend la surveillance et la production de rapports – 20 points 2. Possède des capacités de gestion des comptes d'utilisateur, mais ne comprend pas la surveillance et la production de rapports – 10 points 3. Ne possède aucune capacité de gestion des comptes d'utilisateur – 0 point 	Le soumissionnaire doit démontrer sa conformité en documentant sa capacité de répondre aux exigences, en utilisant des saisies d'écran ou des documents techniques ou d'utilisateur final pour compléter ses réponses.

ID	Exigence	Critères de notation	Justification
R41	<p>Le système proposé par le soumissionnaire doit permettre aux administrateurs du SACAGU d'interroger les comptes d'utilisateur en filtrant sur ce qui suit :</p> <ol style="list-style-type: none"> 1. État des flux de travaux (y compris les tâches attribuées) 2. Dates d'ouverture de session 3. Titre du poste 4. Fonction de gestion des urgences 5. Région / direction générale 6. Secteur d'activités 7. Direction 8. Division 9. Rôle du SACAGU 10. Date d'expiration de l'accès au SACAGU 11. Lieu de travail (c.-à-d. ville, province, numéro civique et nom de rue, étage, numéro de local ou de bureau) 	Chacun des éléments énumérés vaut 1 point, pour un total de 11 points.	Le soumissionnaire doit démontrer sa conformité en documentant sa capacité de répondre aux exigences, en utilisant des saisies d'écran ou des documents techniques ou d'utilisateur final pour compléter ses réponses.
R42	<p>Le système proposé par le soumissionnaire devrait permettre aux utilisateurs du SACAGU de récupérer leur mot de passe en libre-service.</p>	<p>Le système proposé par le soumissionnaire :</p> <ol style="list-style-type: none"> 1. Offre une fonction libre-service de récupération de mot de passe pour les utilisateurs d'EDSC – 10 points 2. Offre une fonctionnalité manuelle de récupération ou de réinitialisation du mot de passe qui doit être effectuée par les administrateurs – 5 points 3. N'offre aucune fonctionnalité de récupération de mot de passe en libre-service pour les utilisateurs d'EDSC – 0 point 	Le soumissionnaire doit démontrer sa conformité en documentant sa capacité de répondre aux exigences, en utilisant des saisies d'écran ou des documents techniques ou d'utilisateur final pour compléter ses réponses.

7.2.1.10.

Interface

utilisateur

ID	Exigence	Critères de notation	Justification
R43	<p>Le système proposé par le soumissionnaire doit posséder les capacités suivantes concernant l'interface utilisateur graphique/tableau de bord :</p> <ol style="list-style-type: none"> 1. Configurabilité selon le type d'utilisateur 2. Visualisation et analyse des points de données du SACAGU (p. ex., plans de continuité des activités achevés, flux de travail exécutés) 	<p>Le système proposé par le soumissionnaire :</p> <ol style="list-style-type: none"> 1. Permet de configurer les interfaces utilisateur graphiques/tableaux de bord en fonction du type d'utilisateur et de visualiser et d'analyser les points de données de service du SACAGU – 10 points 2. Offre la fonctionnalité de visualisation et d'analyse des points de données de service du SACAGU, mais pas de configuration des interfaces utilisateur graphiques/tableaux de bord selon le type d'utilisateur – 5 points 3. Ne comporte aucune fonctionnalité permettant de configurer les interfaces utilisateur graphiques/tableaux de bord ou de visualiser les points de données de service du SACAGU – 0 point 	<p>Le soumissionnaire doit démontrer sa conformité en documentant sa capacité de répondre aux exigences, en utilisant des saisies d'écran ou des documents techniques ou d'utilisateur final pour compléter ses réponses.</p>
R44	<p>Le système proposé par le soumissionnaire doit fonctionner¹ sur :</p>	<p>Le système proposé par le soumissionnaire :</p> <ol style="list-style-type: none"> 1. Peut fonctionner sur des appareils mobiles personnels et 	<p>Le soumissionnaire doit démontrer sa conformité en documentant sa capacité de répondre aux exigences, en utilisant des saisies d'écran ou des documents</p>

ID	Exigence	Critères de notation	Justification
	<ol style="list-style-type: none"> 1. Les appareils mobiles personnels – c.-à-d. connectés directement par l'entremise d'un fournisseur de services Internet; 2. Les appareils mobiles émis par le Canada, connectés par le réseau canadien. <p>¹, y compris la capacité de traiter des données jusqu'au niveau de confidentialité Protégé B.</p>	<p>des appareils émis par le Canada – 10 points</p> <ol style="list-style-type: none"> 2. Peut fonctionner sur des appareils mobiles émis par le Canada ou des appareils personnels – 5 points 3. Ne peut fonctionner sur aucun appareil mobile – 0 point 	techniques ou d'utilisateur final pour compléter ses réponses.
R45	Le soumissionnaire doit confirmer son intention de rendre sa solution SaaS conforme à l'instrument de politique du gouvernement du Canada pour l'accès des appareils mobiles au SaaS pouvant respecter les exigences relatives aux données Protégé B du Canada.	<ol style="list-style-type: none"> 1. Le soumissionnaire confirme son intention – 10 points. 2. Le soumissionnaire ne peut confirmer son intention – 0 point. 	Le soumissionnaire doit démontrer sa conformité en indiquant son intention.
R46	Le système proposé par le soumissionnaire doit permettre de reconnaître les appareils mobiles et de fournir automatiquement le contenu et les fonctionnalités du SACAGU adaptés à l'affichage de l'appareil.	<p>Le système proposé par le soumissionnaire :</p> <ol style="list-style-type: none"> 1. Est capable de reconnaître automatiquement un appareil mobile et de fournir du contenu qui convient le mieux à son affichage – 10 points 2. Est capable de reconnaître automatiquement un appareil mobile, mais ne peut pas fournir le contenu qui convient le mieux à son affichage – 5 points 3. N'est pas capable de reconnaître automatiquement un appareil mobile ni de fournir le contenu qui convient le mieux à son affichage – 0 point 	Le soumissionnaire doit démontrer sa conformité en documentant sa capacité de répondre aux exigences, en utilisant des saisies d'écran ou des documents techniques ou d'utilisateur final pour compléter ses réponses.

ID	Exigence	Critères de notation	Justification
R47	<p>Le système proposé par le soumissionnaire devrait permettre aux utilisateurs du SACAGU de télécharger en toute sécurité¹ des documents et rapports électroniques pour une utilisation hors ligne sur des appareils mobiles et des ordinateurs de bureau.</p> <p>¹ Le téléchargement sécurisé est défini à la section 7.1.1, Tableau 1 – Exigences relatives à la conformité en matière de sécurité.</p>	<p>Le système proposé par le soumissionnaire :</p> <ol style="list-style-type: none"> 1. Peut télécharger des documents pour utilisation hors ligne – 10 points 2. Ne permet pas de télécharger des documents pour utilisation hors ligne – 0 point 	<p>Le soumissionnaire doit démontrer sa conformité en documentant sa capacité de répondre aux exigences, en utilisant des saisies d'écran ou des documents techniques ou d'utilisateur final pour compléter ses réponses.</p>
R48	<p>Le système proposé par le soumissionnaire devrait disposer d'outils d'aide et de formation en ligne pour les utilisateurs du SACAGU, avec leur disponibilité comme suit :</p> <ol style="list-style-type: none"> 1. Conseils sur le positionnement du curseur intégrés au système proposé 2. Fichiers d'aide intégrés ou liés au site Web du soumissionnaire 3. Guides/manuels intégrés ou liés au site Web du soumissionnaire 4. Modules de formation liés au site Web du soumissionnaire 	<p>Chacun des éléments énumérés vaut 3 points, pour un total de 12 points.</p>	<p>Le soumissionnaire doit démontrer sa conformité en documentant sa capacité de répondre aux exigences, en utilisant des saisies d'écran ou des documents techniques ou d'utilisateur final pour compléter ses réponses.</p>

ID	Exigence	Critères de notation	Justification
R49	Le soumissionnaire doit fournir des services de soutien technique aux administrateurs du SACAGU dans la langue canadienne de leur choix par téléphone, courriel, messagerie mobile ou outils Web, selon le cas.	<p>Le soumissionnaire peut fournir des services de soutien technique dans :</p> <ol style="list-style-type: none">1. Les deux langues officielles du Canada – 10 points2. L'une ou l'autre des langues officielles du Canada – 5 points.3. Aucune langue officielle du Canada – 0 point.	

7.2.2. Exigences non fonctionnelles – Cotées

ID	Exigence	Critères de notation	Justification
R50	<p>Le système proposé par le soumissionnaire doit permettre d'importer/exporter des données/de l'information dans les formats de fichier suivants¹ :</p> <ol style="list-style-type: none"> 1. .pdf 2. .doc/.docx 3. .csv 4. .xml 5. .xls 6. .ppt 7. .msg 8. Formats de fichier image : .jpeg ou .tiff ou .bmp ou .png 9. Formats de fichiers vidéo : .mpeg ou .avi ou mp4 10. Formats de fichiers audio : .mp3 ou .wav ou .aiff <p>¹ tout nombre de formats pris en charge dans un élément de liste est compté comme un seul.</p>	Chacun des éléments énumérés vaut 2 points, pour un total de 20 points.	Le soumissionnaire doit démontrer sa conformité en documentant sa capacité de répondre aux exigences, en utilisant des saisies d'écran ou des documents techniques ou d'utilisateur final pour compléter ses réponses.
R51	Le système proposé par le soumissionnaire devrait avoir un temps de disponibilité d'au moins 99 %.	<p>Le service du SACAGU offre un temps de disponibilité de :</p> <ol style="list-style-type: none"> 1. 99,999 % - 10 points 1. > 99,99 % - 8 points 2. > 99,9 % - 6 points 3. = 99 % - 3 points 4. < 99 % - 0 point 	Le soumissionnaire doit démontrer le niveau de conformité dans son entente sur les niveaux de service publiée.

ID	Exigence	Critères de notation	Justification
R52	Le système proposé par le soumissionnaire doit assurer un objectif de point de reprise d'au plus 24 heures en cas de sinistre.	Le système proposé par le soumissionnaire : 1. Peut atteindre un objectif de point de reprise du service du SACAGU de moins de 4 heures – 10 points 2. Peut atteindre un objectif de point de reprise du service du SACAGU de 4 à 8 heures – 8 points 3. Peut atteindre un objectif de point de reprise du service du SACAGU de 8 à 24 heures – 6 points 4. Impossible d'atteindre un objectif de point de reprise du service du SACAGU de 24 heures ou moins – 0 point	Le soumissionnaire doit démontrer le niveau de conformité dans son entente sur les niveaux de service publiée.
R53	Le système proposé par le soumissionnaire doit fonctionner avec les navigateurs de bureau suivants, les versions indiquées ou plus récentes : 1. Internet Explorer v11 2. Microsoft Edge Chromium 93.0.961.47 3. Safari v10 4. Chrome 93.0.4577.82 5. Firefox Quantum 92	Le système proposé par le soumissionnaire : 1. Fonctionne dans tous les navigateurs indiqués – 10 points. 2. Fonctionne dans au moins trois des navigateurs énumérés – 6 points 3. Fonctionne seulement dans Internet Explorer v10 - 3 points 4. Ne fonctionne avec aucun des navigateurs indiqués – 0 point	Le soumissionnaire doit démontrer sa conformité en documentant sa capacité de répondre aux exigences, en utilisant des saisies d'écran ou des documents techniques ou d'utilisateur final pour compléter ses réponses.

ID	Exigence	Critères de notation	Justification
R54	<p>Le système proposé par le soumissionnaire devrait fonctionner dans les navigateurs mobiles compatibles avec les systèmes d'exploitation mobiles suivants :</p> <ol style="list-style-type: none"> 1. Android 2. Système d'exploitation BlackBerry 3. iOS 4. Windows Mobile 	<p>Le système proposé par le soumissionnaire :</p> <ol style="list-style-type: none"> 1. Fonctionne avec des navigateurs mobiles compatibles avec les quatre systèmes d'exploitation mobiles indiqués – 10 points 2. Fonctionne avec des navigateurs mobiles compatibles avec au moins trois des systèmes d'exploitation mobiles indiqués – 5 points 3. Ne fonctionne avec aucun des navigateurs mobiles compatibles avec les systèmes d'exploitation mobiles indiqués – 0 point 	<p>Le soumissionnaire doit démontrer sa conformité en documentant sa capacité de répondre aux exigences, en utilisant des saisies d'écran ou des documents techniques ou d'utilisateur final pour compléter ses réponses.</p>
R55	<p>Le système proposé par le soumissionnaire devrait prendre en charge les fichiers joints d'une taille pouvant atteindre 5 mégaoctets sans avertissement et les fichiers joints de taille supérieure à 5 mégaoctets devraient déclencher un avertissement pour l'utilisateur. Les administrateurs devraient être en mesure de définir les seuils des avertissements.</p>	<p>Le système proposé par le soumissionnaire :</p> <ol style="list-style-type: none"> 1. Prend en charge les pièces jointes et déclenche des avertissements de taille de fichier pour les pièces jointes supérieures à 5 mégaoctets, avec la flexibilité que le seuil soit défini par un administrateur du SACAGU – 10 points 2. Prend en charge les pièces jointes et déclenche des avertissements de taille de fichier pour les pièces jointes supérieures à 5 mégaoctets, mais les seuils ne sont que ceux 	<p>Le soumissionnaire doit démontrer sa conformité en documentant sa capacité de répondre aux exigences, en utilisant des saisies d'écran ou des documents techniques ou d'utilisateur final pour compléter ses réponses.</p>

ID	Exigence	Critères de notation	Justification
		<p>prédéfinis par l'entrepreneur – 8 points</p> <p>3. Prend en charge les pièces jointes de plus de 5 mégaoctets, mais ne peut émettre d'avertissements pour ceux-ci – 6 points</p> <p>4. Ne prend pas en charge les fichiers joints et n'émet pas d'avertissements relatifs à la taille des fichiers – 0 point</p>	
R56	Le système proposé par le soumissionnaire devrait permettre à l'administrateur du SACAGU de configurer une période d'inactivité après laquelle une session d'utilisateur prend fin.	<p>Le système proposé par le soumissionnaire :</p> <p>1. Offre cette fonctionnalité – 10 points</p> <p>2. N'offre pas cette fonctionnalité – 0 point.</p>	Le soumissionnaire doit démontrer sa conformité en documentant sa capacité de répondre aux exigences, en utilisant des saisies d'écran ou des documents techniques ou d'utilisateur final pour compléter ses réponses.
R57	<p>Le soumissionnaire doit offrir au Canada, sans frais supplémentaires, les environnements d'essai suivants :</p> <p>1. Environnement d'essai fonctionnel</p> <p>2. Environnement de mise à l'essai de performance du système</p>	<p>Le soumissionnaire fournira :</p> <p>1. Les deux environnements d'essai – 10 points</p> <p>2. Un seul environnement d'essai – 5 points</p> <p>3. Aucun environnement d'essai – 0 point</p>	Le soumissionnaire doit démontrer sa conformité en documentant sa capacité de répondre aux exigences, en utilisant des saisies d'écran ou des documents techniques ou d'utilisateur final pour compléter ses réponses.
R58	<p>Le soumissionnaire doit fournir une preuve écrite de son engagement à respecter les exigences antérieures et actuelles en matière d'accessibilité des TI qui sont décrites dans les instruments de politique suivants du Canada :</p> <p>1. Loi canadienne sur l'accessibilité</p>	La réponse du soumissionnaire (dans une limite de dix pages) sera évaluée en fonction du degré auquel le soumissionnaire démontre chacun des éléments suivants :	Le soumissionnaire doit démontrer sa conformité en documentant sa capacité à répondre à l'exigence, en utilisant des captures d'écran et/ou de la documentation technique ou de l'utilisateur final pour compléter ses réponses.

ID	Exigence	Critères de notation	Justification
	<p>2. Charte des droits et libertés</p> <p>3. Loi canadienne sur les droits de la personne</p> <p>4. Code canadien du travail, partie II</p> <p>5. Politique sur l'obligation d'accommodement et approbation par le Canada de la Convention relative aux droits des personnes handicapées des Nations Unies</p>	<p>1. Le système proposé par le soumissionnaire a documenté la preuve de la conformité actuelle avec les versions existantes des instruments de politique liés à l'accessibilité des TI répertoriés et le soumissionnaire l'a inclus en réponse au présent énoncé des besoins.–10 points.</p> <p>2. Le système proposé par le soumissionnaire a démontré une évolution continue en ce qui a trait aux normes et aux besoins en matière d'accessibilité des TI. Les délais entre l'introduction de normes nouvelles/mises à jour et la mise en œuvre du produit peuvent aller jusqu'à douze (12) mois–6 points.</p> <p>3. Le soumissionnaire a fait d'importants investissements financiers et organisationnels pour faire progresser son engagement envers l'accessibilité et est un chef de file reconnu de l'industrie et un champion reconnu de l'accessibilité des TI – 3 points.</p> <p>4. Le soumissionnaire n'offre aucun engagement – 0 point.</p>	<p>La preuve de l'engagement du soumissionnaire doit être exprimée par :</p> <p>i. Description détaillée des investissements du soumissionnaire et du leadership public en matière d'accessibilité informatique;</p> <p>ii. Description de la manière dont leur technologie de base a suivi le rythme des normes d'accessibilité informatique, tout au long du cycle de vie de leur produit;</p> <p>iii. Description de la manière dont le système proposé par le soumissionnaire respecte ou dépasse les normes d'accessibilité informatiques existantes (WCAG 2.1, US 508, UE EN 301 549).</p>

Un soumissionnaire sera jugé qualifié pour réussir l'évaluation de la soumission financière s'il obtient au moins 75 % (ou 690) du total maximal des exigences cotées de 920 points.

8. ÉNONCÉ DES TRAVAUX

8.1 Documents de référence

Les documents de référence suivants sont pertinents pour le présent énoncé des travaux :

8.1.1. Le système du soumissionnaire ne doit pas empêcher le Canada (EDSC dans le présent contrat) de s'acquitter de ses obligations décrites dans les instruments de politique suivants du Canada.

1. Gestion des urgences (GU) :
 - i. [Loi sur la gestion des urgences \(2007\)](#)
 - ii. [Politique fédérale en matière de gestion des urgences \(2009\)](#)
 - iii. [Politique sur la sécurité du gouvernement \(2019\)](#)
2. Gestion de la continuité des activités (GCA)
 - i. [Directive sur la gestion de la sécurité - Annexe D : Procédures obligatoires pour le contrôle de la gestion de la continuité des activités \(2019\)](#)
3. Équipes d'urgences et d'évacuation de immeubles (EEUI) :
 - i. [Code canadien du travail \(1985\)](#)
 - ii. [Loi sur les immeubles fédéraux et les biens réels fédéraux \(1991\)](#)
 - iii. [Règlement canadien sur la santé et la sécurité au travail \(2012\)](#)
 - iv. [Norme pour le plan d'évacuation d'urgence et l'organisation des secours en cas d'incendie — Chapitre 3.1 du Conseil du Trésor \(1994\)](#)
4. Protection contre les incendies :
 - i. [Norme sur la protection contre les incendies du Conseil du Trésor \(2019\)](#)
 - ii. [Code national de prévention des incendies \(2010\)](#)
 - iii. [Code national du bâtiment — Canada \(2010\)](#)
 - iv. [Politique du Conseil du Trésor sur la gestion des biens immobiliers \(2019\)](#)

Le système proposé par le soumissionnaire ne devrait pas empêcher le Canada de se conformer aux instruments de politique suivants :

5. [Loi sur l'accès à l'information](#)
6. [Loi sur les langues officielles](#)
7. [Loi sur la protection des renseignements personnels](#)
8. [Directive sur la gestion des communications](#)
9. [Politique sur l'accès à l'information](#)
10. [Politique sur la gestion de l'information](#)
11. [Règles pour l'accessibilité des contenus Web \(WCAG\) 2.0 \(en anglais seulement\)](#)
12. [Lignes directrices concernant la conservation des documents administratifs communs de l'administration fédérale](#)
13. [Norme sur la facilité d'emploi des sites Web](#)
14. [Boîte à outils de l'expérience Web – Ligne directrice](#)
15. [Normes sur la protection de la vie privée et le Web analytique](#)
16. [Loi sur le ministère de l'Emploi et du Développement social](#)
17. [Loi sur la Bibliothèque et les Archives du Canada](#)
18. [Norme sur l'assurance de l'identité et des justificatifs](#)
19. [Norme sur le filtrage de sécurité](#)
20. [Algorithmes cryptographiques pour les renseignements non classifiés, Protégé A et Protégé B](#)
21. [Norme sur les métadonnées](#)
22. [Directive sur la tenue de documents](#)

8.2 Portée des travaux

Au moment de l'attribution du contrat et avant que le Canada accepte le système mis en œuvre, l'entrepreneur doit exécuter les travaux suivants :
L'entrepreneur devra fournir les travaux et services suivants, conformément aux plans acceptés par le Canada et énumérés dans le tableau 2 ci-dessous.

Les travaux à effectuer et les services à fournir entre la signature du contrat et la mise en production sont les suivants :

- 8.2.1 Une fois l'abonnement payé pour les 20 utilisateurs principaux initiaux, créer un accès au système (comptes d'utilisateur) pour ceux-ci
- 8.2.2 Former les 20 utilisateurs principaux
- 8.2.3 Configurer le SACAGU
- 8.2.4 Assurer la migration des actifs informationnels du Canada vers le SACAGU
- 8.2.5 Une fois l'abonnement payé pour les 2 980 autres utilisateurs, créer un accès au système (comptes d'utilisateur) pour ceux-ci
- 8.2.6 Si l'entrepreneur l'offre au Canada, établir les environnements d'essai fonctionnel et de rendement du SACAGU
- 8.2.7 Si des environnements d'essai sont configurés, mettre à l'essai la fonctionnalité et le rendement du SACAGU, au besoin et sur demande au moyen du processus d'autorisation de tâches
- 8.2.8 Aider le Canada à former les 2 980 autres utilisateurs, sur demande, dans le cadre du processus d'autorisation des tâches
- 8.2.9 Aider au déploiement du service du SACAGU, sur demande, dans le cadre du processus d'autorisation des tâches.
- 8.2.10 Fournir des services de dépannage, au besoin
- 8.2.11 Fournir des services de soutien technique, au besoin

Les travaux à effectuer et les services à fournir après la production et pendant la durée du contrat sont les suivants :

- 8.2.12 Fournir des services de dépannage (bilingues), au besoin
- 8.2.13 Fournir des services de soutien technique (bilingues), au besoin

Dans chacun des plans énumérés ci-dessous, l'entrepreneur inclura un calendrier interne des activités pertinentes en ce qui a trait à la date d'attribution du contrat.

Au moment de l'attribution du contrat, le Canada présidera une petite série de réunions de lancement de projet au cours desquelles il l'entrepreneur et où les échéanciers des plans soumis pourront être rajustés afin d'être intégrés à un calendrier de projet final.

On s'attend à ce que l'entrepreneur fournisse des ressources qualifiées pour fournir un service de qualité dans les délais mutuellement convenus précisés dans les plans acceptés.

Tableau 2 – Calendrier des produits livrables

N°	Titre du produit livrable	Description du produit livrable	Type de produit livrable	Date d'échéance
8.3.1	Plan de formation sur le SACAGU	<p>Le plan doit veiller à ce que la formation soit suffisamment complète pour que les stagiaires du Canada puissent :</p> <ul style="list-style-type: none"> i. Utiliser toutes les caractéristiques fonctionnelles et administratives; ii. Configurer et adapter le SACAGU; iii. Migrer les actifs informationnels existants; iv. Fournir une assistance technique aux autres utilisateurs du Canada. <p>Le soumissionnaire proposera les meilleures façons d'offrir la formation relativement à l'emplacement au Canada. Au moment de l'attribution du contrat, l'entrepreneur et le Canada pourraient devoir faire des mises à jour avant que le Canada accepte le plan final.</p>	Document	Soumettre avec la soumission.
8.3.2	Plan de mise en œuvre du SACAGU	<p>Le plan doit décrire la façon dont l'entrepreneur envisage toutes les activités pertinentes à la mise en œuvre, sans se limiter à ce qui suit :</p> <ul style="list-style-type: none"> i. Création d'un accès au système pour les utilisateurs; ii. Configuration du SaaS générique de l'entrepreneur dans le SACAGU en tant que service du Canada (c.-à-d. service du GC); 	Document	Soumettre avec la soumission.

N°	Titre du produit livrable	Description du produit livrable	Type de produit livrable	Date d'échéance
		<p>iii. Migration des actifs informationnels du Canada vers le SACAGU;</p> <p>iv. Transfert et synchronisation avec le SACAGU des données de la plateforme de gestion de l'identité du Canada (Microsoft Active Directory) nécessaires à l'authentification de l'accès au système;</p> <p>v. Activation du SACAGU pour recevoir les mises à jour hebdomadaires d'EDSC de certaines données sur le personnel sous forme de fichier CSV chiffré.</p> <p>Au moment de l'attribution du contrat, l'entrepreneur et le Canada pourraient devoir faire des mises à jour avant que le Canada accepte le plan final.</p>		Finaliser après les ateliers de lancement.
8.3.3	Plan de réalisation des tests pour le SACAGU	<p>Le plan doit décrire la façon dont l'entrepreneur envisage au moins les activités suivantes :</p> <p>i. Définition et configuration de tous les environnements d'essai offerts;</p> <p>ii. Définition des types d'essai offerts (p. ex., fonctionnel, rendement) et identification des rôles (entrepreneur et Canada) pour chaque type d'essai.</p> <p>iii. Définition des cas d'essai et moment estimé de leur exécution.</p> <p>iv. Au moment de l'attribution du contrat, l'entrepreneur et le Canada pourraient devoir faire des mises à jour avant que le Canada accepte le plan final.</p>	Document	<p>Soumettre avec la soumission.</p> <p>Finaliser après les ateliers de lancement.</p>
8.3.4	Plan de déploiement du SACAGU	<p>Le plan doit décrire la façon dont l'entrepreneur envisage la mise en œuvre auprès de 3 000 utilisateurs formés.</p> <p>Au moment de l'attribution du contrat, l'entrepreneur et le Canada pourraient devoir faire des mises à jour avant que le Canada accepte le plan final.</p>	Document	<p>Soumettre avec la soumission.</p> <p>Finaliser après les ateliers de lancement.</p>
8.3.5	Réunions de lancement du projet	L'entrepreneur participera à la série de réunions de type atelier présidées par le Canada, au cours desquelles il discutera et conviendra de plus amples	Réunions	Commencer dans les cinq jours ouvrables suivant la

N°	Titre du produit livrable	Description du produit livrable	Type de produit livrable	Date d'échéance
		détails sur les produits livrables susmentionnés et leur calendrier d'exécution. L'entente entraînera probablement une certaine modification des échéanciers fournis par l'entrepreneur dans ses plans soumis afin de les harmoniser avec le calendrier global prévu du projet.		signature du contrat.
8.3.6	Accès au système pour 20 utilisateurs principaux	Après 20 abonnements payés, il faut créer un accès au système (comptes d'utilisateur) pour les 20 premiers utilisateurs.	Comptes d'utilisateurs	Dans les trois jours ouvrables suivant la signature du contrat.
8.3.7	Plan de continuité des activités du SACAGU et plan de reprise après sinistre	Les plans doivent comprendre au moins les renseignements suivants : i. Le temps de reprise après une interruption; ii. Le temps nécessaire pour passer à un site de sauvegarde; iii. Le niveau de service et la fonctionnalité fournis par le site de sauvegarde et période pendant laquelle le répondant récupérera les données primaires et le service principal; iv. Rapport sur la méthode et la fréquence à laquelle l'entrepreneur met à l'essai ou exerce ces plans L'entrepreneur et le Canada pourraient devoir faire des mises à jour avant que le Canada accepte le plan final.	Document	Soumettre dans les dix jours ouvrables suivant la date d'attribution du contrat.
8.3.8	Guide de l'administrateur du SACAGU	Le guide doit décrire tout ce qu'un administrateur du SACAGU doit accomplir dans ce rôle. L'entrepreneur et le Canada pourraient devoir faire des mises à jour avant que le Canada accepte le plan final.	Document	Soumettre dans les dix jours ouvrables suivant l'attribution du contrat.
8.3.9	Guide de l'utilisateur du SACAGU	Le guide doit décrire tout ce qui est nécessaire pour qu'un utilisateur du SACAGU puisse utiliser ce service conformément à ce qui est défini dans l'énoncé des besoins. L'entrepreneur et le Canada pourraient devoir faire des mises à jour avant que le Canada accepte le plan final.	Document	Soumettre dix jours ouvrables après l'attribution du contrat.

N°	Titre du produit livrable	Description du produit livrable	Type de produit livrable	Date d'échéance
8.3.10	Formation de base	Guidé par le plan de formation du SACAGU, l'entrepreneur doit former 20 utilisateurs principaux afin qu'ils deviennent des administrateurs du SACAGU, qui pourront alors : - aider l'entrepreneur à configurer le SACAGU et à migrer ses actifs informationnels; - effectuer des essais fonctionnels et de rendement (si des environnements d'essai sont offerts au Canada); - former les 2 980 autres utilisateurs.	Services professionnels	Le début et la durée seront conformes au plan de formation du SACAGU accepté par le Canada; le Canada prévoit que la durée sera d'au plus cinq jours ouvrables.
8.3.11	Configuration du SACAGU	Guidé par le plan de mise en œuvre du SACAGU, l'entrepreneur doit configurer son SaaS dans le SACAGU pour devenir un service du Canada (c.-à-d. un service du GC). La configuration sera effectuée de manière à satisfaire aux exigences énoncées dans l'énoncé des besoins pour lesquelles le soumissionnaire a affirmé qu'il se conformait. La configuration doit être effectuée dans les délais prévus dans le calendrier principal du projet du Canada, harmonisée avec les ressources désignées de l'entrepreneur, qualifiées pour configurer le SaaS commercial dans le SACAGU du Canada, exécutera cette activité dans le cadre de ses services de mise en œuvre et de configuration. Il n'y aura pas de rappel pour cette activité et l'entrepreneur peut choisir de préciser les frais séparément ou dans le cadre des frais d'abonnement. L'entrepreneur pourrait vouloir définir son processus de choix dans le plan de mise en œuvre du SACAGU afin d'éclairer le plan final accepté par le Canada.	Services professionnels	Le début et la durée seront conformes au plan de mise en œuvre du SACAGU accepté par le Canada. Le Canada estime que la durée ne peut pas dépasser 15 jours ouvrables.
8.3.12	Migration des actifs informationnels du Canada	Guidé par le plan de mise en œuvre du SACAGU, l'entrepreneur doit migrer les ressources d'information du Canada (données et information existantes, données de la plateforme de gestion de l'identité du Canada (fondée sur Microsoft Active Directory) nécessaires à l'authentification des utilisateurs).	Services professionnels	Le début et la durée seront conformes au plan de mise en œuvre du SACAGU accepté par le Canada. Le Canada estime qu'il

N°	Titre du produit livrable	Description du produit livrable	Type de produit livrable	Date d'échéance
		<p>La migration doit être effectuée dans les délais prévus dans le calendrier principal du projet du Canada, conformément au plan de mise en œuvre du SACAGU accepté par le Canada.</p> <p>Les ressources désignées de l'entrepreneur, qualifiées pour migrer les actifs informationnels du Canada au SACAGU du Canada, exécuteront cette activité dans le cadre de leurs services de mise en œuvre ou de configuration.</p> <p>Il n'y aura pas de rappel pour cette activité et l'entrepreneur peut choisir de préciser les frais séparément ou dans le cadre des frais d'abonnement.</p> <p>L'entrepreneur pourrait vouloir définir son processus de choix dans le plan de mise en œuvre du SACAGU afin d'éclairer le plan final accepté par le Canada.</p>		ne durera pas plus de 20 jours ouvrables.
8.3.13	Mise à l'essai du SACAGU – Fonctionnel et rendement	<p>Guidé par le plan d'essai du SACAGU, l'entrepreneur doit :</p> <ul style="list-style-type: none"> i. (s'ils sont offerts au Canada dans leur soumission) Établir des environnements d'essai pour les essais fonctionnels et de rendement; ii. Être disponible au Canada et aider au besoin à effectuer les essais fonctionnels et de rendement de l'application logicielle (service). <p>Les ressources désignées par l'entrepreneur et qualifiées pour soutenir le Canada en ce qui concerne les essais seront sollicitées uniquement si le Canada fait face à des problèmes qu'il ne peut résoudre lui-même. Le temps consacré par la ressource de l'entrepreneur sera surveillé par l'État et une fois les essais terminés, il sera approuvé par le Canada pour être facturé à l'heure. L'entrepreneur pourrait vouloir définir son processus de choix dans le plan d'essai du SACAGU afin d'éclairer le plan final accepté par le Canada.</p>	Services professionnels	Le début et la durée seront conformes au plan d'essai du SACAGU accepté par le Canada. Le Canada estime qu'il ne durera pas plus de 35 jours ouvrables.
8.3.14	Accès au système pour les 2 980 autres utilisateurs	Sur paiement pour les 2 980 abonnements, l'entrepreneur doit créer un accès au système (comptes d'utilisateur) pour les 2 980 autres utilisateurs.	Services professionnels	Le début et la durée seront conformes au plan de mise en œuvre du SACAGU,

N°	Titre du produit livrable	Description du produit livrable	Type de produit livrable	Date d'échéance
		Cette activité doit se dérouler dans les délais prévus dans le calendrier principal du projet du Canada, conformément au plan de mise en œuvre du SACAGU accepté par le Canada.		accepté par le Canada. Le Canada estime qu'il ne durera pas plus de dix jours ouvrables.
8.3.15	Formation de masse des utilisateurs	<p>Guidé par le plan de formation du SACAGU, l'entrepreneur doit appuyer le Canada, au besoin, dans la prestation de la formation aux autres utilisateurs.</p> <p>Les formateurs désignés du Canada, eux-mêmes formés à titre de 20 utilisateurs principaux, offriront la formation aux autres utilisateurs. Les ressources désignées de l'entrepreneur, qualifiées pour appuyer le Canada en matière de formation, ne seront sollicitées que si le Canada fait face à des problèmes qu'il ne peut résoudre lui-même. Le temps consacré par la ressource de l'entrepreneur sera surveillé par l'État et une fois la formation terminée, il sera approuvé par le Canada pour être facturé à l'heure. L'entrepreneur pourrait vouloir définir son processus de choix dans le plan de formation du SACAGU afin d'éclairer le plan final accepté par le Canada.</p>	Services professionnels	Le début et la durée seront conformes au plan de formation du SACAGU accepté par le Canada. Le Canada estime qu'il pourrait ne pas durer plus de 60 jours ouvrables.
8.3.16	Déploiement du SACAGU	<p>Guidé par le plan de déploiement du SACAGU, l'entrepreneur doit déployer le service du SACAGU auprès de tous les autres utilisateurs définis (soit 2 980 utilisateurs).</p> <p>Cette activité doit se dérouler dans les délais prévus dans le calendrier principal du projet du Canada, conformément au plan de déploiement du SACAGU accepté par le Canada.</p> <p>Les ressources désignées par l'entrepreneur, qualifiées pour soutenir le Canada dans le cadre du déploiement, ne seront sollicitées que si le Canada fait face à des problèmes qu'il ne peut résoudre lui-même. Le temps consacré par la ressource de l'entrepreneur sera surveillé par l'État et une fois la formation terminée, il sera approuvé par le Canada pour être facturé à l'heure. L'entrepreneur pourrait vouloir définir son processus de choix dans le plan de déploiement du SACAGU afin d'éclairer le plan final accepté par le Canada.</p>	Services professionnels	<p>Le début et la durée seront conformes au plan de déploiement du SACAGU accepté par le Canada.</p> <p>Le Canada suppose qu'un utilisateur ne peut être déployé avant d'avoir reçu une formation.</p> <p>Le Canada estime que le déploiement complet de</p>

N°	Titre du produit livrable	Description du produit livrable	Type de produit livrable	Date d'échéance
8.3.17	Entrée en service	<p>L'entrepreneur doit aider le Canada, au besoin, à mettre le SACAGU en service.</p> <p>Les ressources désignées par l'entrepreneur, qualifiées pour soutenir le Canada en ce qui concerne le lancement de la production, seront sollicitées uniquement si le Canada fait face à des problèmes qu'il ne peut résoudre lui-même. Le temps consacré par la ressource de l'entrepreneur sera surveillé par l'État et une fois la formation terminée, il sera approuvé par le Canada pour être facturé à l'heure. L'entrepreneur pourrait vouloir définir son processus de choix dans le plan de déploiement du SACAGU afin d'éclairer le plan final accepté par le Canada.</p>	Services professionnels	2 980 utilisateurs pourrait ne pas durer plus de 30 jours ouvrables.
				Début à l'achèvement du déploiement (mais au plus tard une semaine après celui-ci) et après l'obtention de l'autorisation d'exploitation; dure un jour ouvrable.

8.4 Appui fourni par EDSC

Dans ses locaux au Canada, le Canada fournira l'équipement informatique et la connectivité réseau adéquate au SACAGU ainsi que la bande passante requise pour la formation sur place de ses utilisateurs désignés comme administrateurs du SACAGU.

Le Canada déterminera, en consultation avec l'entrepreneur, quelles données et/ou informations et quels documents de référence pertinents seront nécessaires pour mener à bien la formation de base et fournira les éléments convenus.

8.5 Contraintes

L'entrepreneur doit tenir compte des contraintes suivantes du projet et s'y conformer :

- 8.5.1 L'entrepreneur doit fournir les documents énumérés à la section 3.1 et tout autre document jugé conjointement par l'entrepreneur et le Canada comme nécessaire à l'exécution réussie des tâches énumérées, en anglais et en français, en version électronique, à l'adresse de l'autorité contractante du SACAGU précisée dans le document principal de la DP.

8.5.2 L'entrepreneur n'aura aucun accès physique à aucun des sites du Canada faisant partie du réseau du Canada. L'entrepreneur peut avoir accès, physiquement ou à distance, à l'instance du SACAGU du Canada dans son nuage public, mais seulement pour le personnel ayant reçu le contrôle sécuritaire adéquat de personnel du Canada. Pour plus de détails, veuillez consulter la section Exigences relatives à la sécurité de l'énoncé des besoins et le document principal de la DP.

Annexe A – Glossaire

Terme	Définition
NVSA	Norme de vérification de la sécurité des applications
GCA	Gestion de la continuité des activités
PCA	Plan de continuité des activités
PEUI	Plans d'évacuation d'urgence des immeubles
ARA	Analyse des répercussions sur les activités
CCC	Centre canadien pour la cybersécurité (anciennement appelé CST ou CSTC)
MCN	Matrice des contrôles du nuage
CIS	Centre for Internet Security
BDGC	Base de données de la gestion de la configuration
DGC	Équipe de gestion de crises
RCR	Réanimation cardio-respiratoire
CSA	Cloud Security Alliance
CST	Centre de la sécurité des télécommunications (anciennement appelé CCCS)
CSTC	Centre de la sécurité des télécommunications Canada
FSI	Fournisseur de services infonuagiques – fournisseur d'un ou de plusieurs services infonuagiques (IaaS, PaaS, SaaS)
CSV	Fichiers de valeurs séparées par des virgules
GU	Gestion des urgences
SACAGU	Système d'application de continuité des activités et de gestion des urgences
EDSC	Emploi et Développement social Canada, un ministère du gouvernement du Canada
PFIU	Plan fédéral d'intervention d'urgence
NFTI	Normes fédérales de traitement de l'information
CANADA	Gouvernement du Canada, pour la présente demande de soumissions, désigne également EDSC
IaaS	Infrastructure comme service
ISO	Organisation internationale de normalisation
TI	Technologie de l'information
GCSTI	Gestion de la continuité des services de technologie de l'information
TAMA	Temps d'arrêt maximal admissible

Terme	Définition
NIST	National Institute of Standards and Technology
OWASP	Open Web Application Security Project
PaaS	Plateforme comme service
PBMM	Protégé B, intégrité moyenne, disponibilité moyenne
ICR	Indicateurs clés de rendement
OPR	Objectif de point de reprise
ODR	Objectif de délai de rétablissement
SaaS	Logiciels en tant que service
SAFECode	Forum sur l'assurance logicielle pour l'excellence du Code
SAML	Langage de balisage des assertions de sécurité (Security Assertion Markup Language)
ICA	Intégration des chaînes d'approvisionnement
GRCA	Gestion des risques liés à la chaîne d'approvisionnement
ENS	Entente sur les niveaux de service
PON	Procédure opérationnelle normalisée
TLS	Protocole TLS (Transport Layer Security)
RPV	Réseau privé virtuel

Annexe B – Glossaire

Terme	Définition
Actifs	Les actifs comprennent, sans s'y limiter, l'information de toute forme et les médias, les réseaux, les systèmes, le matériel, les biens réels, les ressources financières, les fiduciaires d'employés, la confiance du public et la réputation internationale. (Guide pour la planification de la gestion des urgences 2010-2011 de Sécurité publique Canada)
Sensibilisation	Favoriser une compréhension des problèmes et les limites de base de la GCA. Cela permettra au personnel de reconnaître les menaces et de réagir en conséquence. La distribution d'affiches et de dépliants destinés à l'ensemble de l'entreprise ou la tenue de séances d'information précises sur la continuité des activités à l'intention de la haute direction de l'entreprise sont des exemples de cette sensibilisation. La sensibilisation est moins formelle que la formation et vise généralement l'ensemble du personnel.
Direction générale	Une subdivision de premier niveau d'EDSC.
Gestion de la continuité des activités (GCA)	Processus de gestion global qui permet de cerner les menaces potentielles pour une organisation et les répercussions que ces menaces pourraient causer sur les activités opérationnelles, et qui fournit un cadre pour renforcer la résilience organisationnelle et la capacité d'intervention efficace qui protège les intérêts de ses principaux intervenants, la réputation, la marque et les activités de création de valeur.
Plan de continuité des activités (PCA)	Un ensemble documenté de procédures et de renseignements qui est élaboré, compilé et tenu à jour en vue d'une utilisation en cas d'incident pour permettre à une organisation de continuer d'offrir ses produits et services essentiels à un niveau acceptable prédéfini.
Analyse des répercussions sur les activités (ARA)	Une méthode de détermination des conséquences d'un défaut d'exécution d'une fonction ou d'une exigence.
Liste de vérification	1. Outil pour rappeler ou valider que les tâches ont été accomplies et que des ressources sont disponibles pour rendre compte de l'état du rétablissement. 2. Liste des éléments (noms ou tâches, etc.) à vérifier ou à consulter.
Services infonuagiques	Services habituellement inclus dans les modèles de services infonuagiques comme SaaS, PaaS ou IaaS.
Risques liés à la conformité	Les risques liés à la conformité concernent la conformité juridique et réglementaire.
Base de données de la gestion de la configuration	Base de données utilisée par une organisation pour stocker des renseignements sur le matériel et les logiciels (communément appelés éléments de configuration). Cette base de données sert d'entrepôt de données pour l'organisation et conserve également des renseignements sur les relations entre ses actifs.
Plan de rechange	Plan utilisé par une organisation ou une unité opérationnelle pour réagir à une panne de système particulière ou à une interruption des activités.

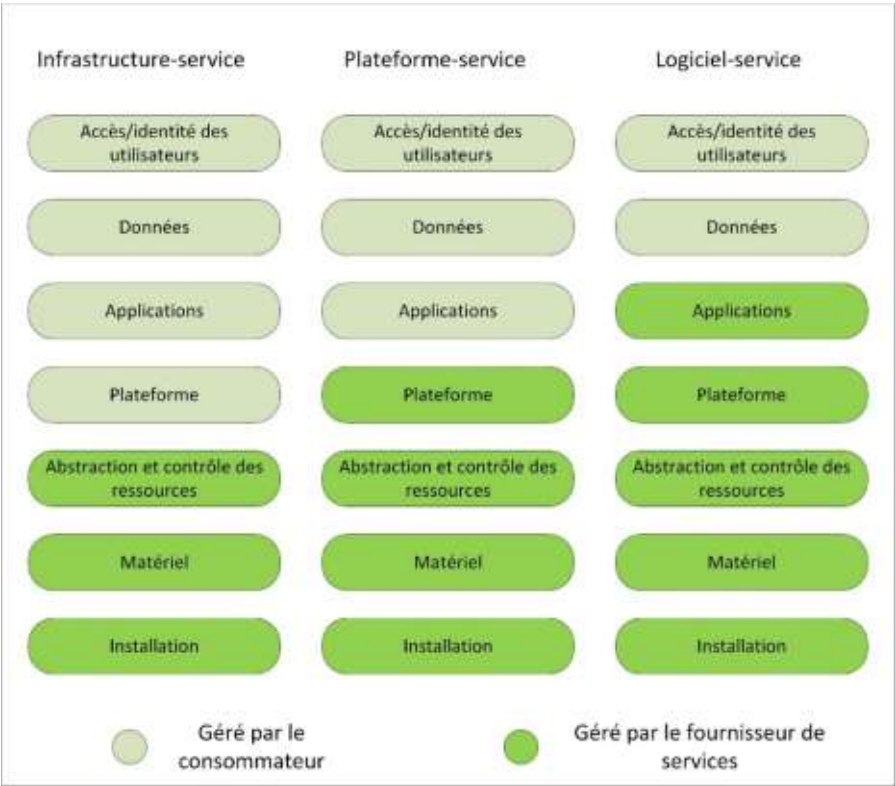
Terme	Définition
Gestion de crise	Coordination globale de l'intervention d'une organisation en cas de crise, de manière efficace et en temps opportun, dans le but d'éviter ou de minimiser les dommages à la rentabilité, à la réputation et à la capacité d'exploitation de l'organisation.
L'équipe de gestion de crise (EGC)	Groupe de personnes chargées d'élaborer et de mettre en œuvre un plan complet d'intervention en cas d'incident perturbateur. L'équipe se compose d'un groupe central de décideurs formés en gestion des incidents et prêts à réagir à toute situation.
Direction	Subdivision de premier niveau d'une direction générale.
Planification de la reprise après sinistre	Activités associées à la disponibilité continue et à la planification de la restauration de l'infrastructure de TI.
Division	Subdivision de premier niveau d'une direction.
Documents électroniques	Tout document stocké par le SACAGU. Comprend les plans, les rapports, les listes de vérification, les questionnaires, les listes, les calendriers et les modèles de gestion des urgences.
Administrateur du SACAGU	Rôle du SACAGU, un rôle ayant les privilèges les plus élevés pour l'utilisation du système, y compris la gestion des comptes d'utilisateur.
Guide de l'administrateur du SACAGU	Guide adapté au type d'utilisateur de l'administrateur du SACAGU.
Contributeur au SACAGU	Rôle du SACAGU, un rôle comportant des privilèges limités, habituellement dans un domaine opérationnel particulier.
Coordonnateur du SACAGU	Rôle du SACAGU, avec les privilèges les plus élevés, mais pour un domaine opérationnel particulier.
Calendrier du projet du SACAGU	Calendrier de projet élaboré par le CANADA, en consultation avec le fournisseur.
Guide de l'utilisateur du SACAGU	Guide adapté aux autres types d'utilisateurs du SACAGU, comme le coordonnateur du SACAGU, le contributeur du SACAGU, le visualiseur du SACAGU.
Visualiseur du SACAGU	Rôle du SACAGU, un rôle comportant uniquement des droits d'accès en lecture seule.
Gestion des urgences (GU)	<ol style="list-style-type: none"> Processus continu de prévention, d'atténuation, de préparation, d'intervention, de continuité et de reprise après un incident qui menace la vie, les biens, les opérations ou l'environnement. (NFPA 1600) Programme qui met en œuvre la mission, la vision, les buts stratégiques, les objectifs et le cadre de gestion du programme et de l'organisation.
Activités de gestion des urgences (GU)	<p>Cela inclut :</p> <ol style="list-style-type: none"> Exercices d'urgence <ol style="list-style-type: none"> Continuité des activités Gestion des urgences Continuité de la TI Cycles de création et d'examen des documents électroniques Formation de l'équipe d'évacuation d'urgence de l'immeuble Activités de sensibilisation à la gestion des urgences
Plans de gestion des urgences	<p>Cela inclut :</p>

Terme	Définition
	<ol style="list-style-type: none"> 1. Plan de continuité des activités (PCA) 2. Analyse des répercussions sur les activités (ARA) 3. Continuité de la TI 4. Plan d'évacuation d'urgence de l'immeuble (PEUI) 5. Plans d'urgence 6. Plans d'action
Emploi et Développement social Canada (EDSC)	Un ministère du gouvernement du Canada qui sollicite un système dans le cadre de cet approvisionnement.
Exercice	Activité au cours de laquelle le ou les plans de l'entité sont mis en œuvre en tout ou en partie pour s'assurer qu'ils contiennent l'information appropriée et produisent le résultat souhaité lorsqu'ils sont mis en œuvre.
Exercices à grande échelle	Un exercice à grande échelle est un exercice multi-organismes, multijuridictionnel et multidisciplinaire faisant appel à des fonctions (p. ex., bureau conjoint sur le terrain, centres des opérations d'urgence) et à des interventions « sur le terrain » (p. ex., des employés de la continuité qui déménagent dans leurs autres sites pour exécuter des fonctions essentielles axées sur des scénarios).
Incidence sur le bien-être économique des Canadiens/du public	Comprend les services économiques, monétaires et financiers essentiels et fondamentaux requis pour maintenir la sécurité du revenu, la stabilité économique, les services bancaires essentiels et les programmes de prestations parrainés par le gouvernement requis pour maintenir le mieux-être des Canadiens et éviter un préjudice élevé.
Incidence sur le fonctionnement du gouvernement ou de l'organisation	Comprend les services gouvernementaux essentiels, les accords constitutionnels, les programmes, les politiques, les règlements, la législation et l'affectation des ressources humaines et financières requises pour maintenir l'efficacité du gouvernement et éviter un préjudice élevé.
Incidence sur la santé des Canadiens/du public	Renvoie aux services « de soins et d'intervention d'urgence » requis pour assurer la subsistance et pour éviter les blessures. Cela comprend les services d'urgence nécessaires pour sauver des vies et pour rétablir le « fonctionnement » normal des personnes à la suite d'un traumatisme ou d'un accident grave.
Incidence sur la conformité juridique et réglementaire du Ministère/organisme	Comprend la législation, la politique directrice, les litiges et les obligations (PE, ententes, traités, contrats, clients internes/externes).
Incidence sur la confiance et la réputation du public dans le Ministère ou l'organisation	Renvoie à l'évaluation subjective que fait la population de la crédibilité du gouvernement et de sa capacité d'offrir des services.
Incidence sur la sûreté des Canadiens/du public	Comprend les services essentiels (comme les services d'incendie, la police, les ambulances) et les services de sécurité généraux (y compris la sécurité nucléaire, l'intervention en cas de déversement de matières dangereuses, l'atténuation des effets d'une contamination chimique, biologique, radiologique ou nucléaire, les services de recherche et sauvetage, la sécurité des immeubles, des lieux publics et des rassemblements publics) requis pour maintenir un environnement de maintien de la vie, pour assurer la subsistance et pour protéger la sécurité des personnes, afin d'éviter un préjudice élevé.

Terme	Définition
Incidence sur la sécurité des Canadiens/du public	Comprend les services essentiels requis pour maintenir l'ordre public, les communications et le transport essentiels, la poursuite des activités du gouvernement, l'intégrité territoriale et la souveraineté de la nation, la sûreté des immeubles, des lieux publics et des rassemblements publics, et la sûreté des Canadiens, afin d'éviter un préjudice élevé.
Incident	Événement susceptible de causer une interruption, une perturbation, une perte, une urgence, une crise, un sinistre ou une catastrophe.
Gestion des incidents	Processus par lequel une organisation intervient et contrôle un incident au moyen de procédures ou de plans d'intervention d'urgence.
Plan d'intervention en cas d'incident	Documentation d'un ensemble prédéterminé d'instructions ou de procédures pour détecter un incident, y réagir et en limiter les conséquences pour les systèmes de TI de l'organisation.
Technologie de l'information (TI)	Utilisation de la technologie pour le stockage, la communication ou le traitement de l'information. La technologie comprend généralement des ordinateurs, des télécommunications, des applications et d'autres logiciels. Les renseignements peuvent inclure des données opérationnelles, de la voix, des images, des vidéos, etc. La technologie de l'information est souvent utilisée pour appuyer les processus opérationnels par l'entremise des services de TI.
Infrastructure comme service (IaaS)	La capacité fournie au consommateur consiste à fournir des services de traitement, de stockage, de réseaux et d'autres ressources informatiques fondamentales permettant au consommateur de déployer et d'exécuter des logiciels arbitraires, notamment des systèmes d'exploitation et des applications. Le consommateur ne gère ni ne contrôle l'infrastructure informatique sous-jacente, mais exerce un contrôle sur les systèmes d'exploitation, le stockage et les applications déployées, et peut-être un contrôle limité de certaines composantes de réseautage (p. ex., pare-feu hébergés).
Gestion de la continuité des services de TI (GCSTI)	Processus responsable de la gestion des risques qui pourraient avoir une incidence importante sur les services de TI. Le GCSTI veille à ce que le fournisseur de services de TI puisse toujours fournir des niveaux de service minimaux convenus, en réduisant le risque à un niveau acceptable et en planifiant le rétablissement des services de TI. Le GCSTI devrait être conçu pour appuyer la gestion de la continuité des activités.
Temps d'arrêt maximal acceptable	Temps maximum écoulé entre une interruption et le rétablissement de la capacité opérationnelle requise.
Plateforme comme service (PaaS)	La capacité fournie au consommateur consiste à déployer dans l'infrastructure informatique les applications créées ou acquises par le consommateur et créées au moyen de langages de programmation, de bibliothèques, de services et d'outils soutenus par le fournisseur. Le consommateur ne gère ni ne contrôle l'infrastructure informatique sous-jacente, y compris le réseau, les serveurs, les systèmes d'exploitation ou le stockage, mais il contrôle les applications déployées et peut-être les paramètres de configuration de l'environnement d'hébergement des applications.
Protégé A	Classification canadienne de la confidentialité des données, c'est-à-dire que leur divulgation non autorisée pourrait causer un préjudice, par exemple une atteinte à la vie privée ou de l'embarras.

Terme	Définition
Protégé B	Classification canadienne de la confidentialité des données, c'est-à-dire que leur divulgation non autorisée pourrait causer un préjudice grave à des intérêts privés ou autres intérêts non nationaux, à une personne ou à une entreprise, comme une atteinte à la vie privée ou un embarras.
RACI	Matrice de propriété des risques, acronyme signifiant Responsable-Imputable-Consulté-Informé
Objectif de point de reprise (OPR)	Point où l'information utilisée par une activité doit être restaurée pour permettre à l'activité de fonctionner à la reprise. Remarque de l'éditeur concernant ISO : On peut aussi parler de « perte maximale de données ».
Objectif de délai de reprise (ODR)	Délai fixé pour le rétablissement et la reprise des fonctions ou des ressources en fonction du temps d'arrêt acceptable et du niveau de rendement acceptable en cas d'interruption des activités.
Région	Une subdivision d'EDSC ventilée selon les frontières géographiques définies par EDSC. Au moment de la rédaction, EDSC comptait cinq régions.
Rapports	Ils comprennent les rapports après action, les journaux d'audit, les rapports de situation, les rapports spéciaux, la liste de vérification des inspections d'étages et les listes de personnes-ressources.
Risque	Événement possible qui pourrait causer des préjudices ou des pertes, ou nuire à la capacité d'atteindre les objectifs. Un risque est mesuré par la probabilité d'une menace, la vulnérabilité de l'actif face à cette menace et l'impact qu'elle produirait s'il survenait.
Évaluation des risques	Processus d'identification des risques pour une organisation, d'évaluation des fonctions essentielles nécessaires à la poursuite des activités opérationnelles, de définition des contrôles en place pour réduire l'exposition de l'organisation et d'évaluation du coût de ces contrôles. L'analyse des risques consiste souvent à évaluer les probabilités d'un événement particulier.
Logiciel en tant que service (SaaS)	La capacité fournie au consommateur consiste à utiliser les applications du fournisseur fonctionnant sur une infrastructure infonuagique. Les applications sont accessibles à partir de divers appareils du client au moyen d'une interface client mince, comme un navigateur Web (p. ex., courriel Web) ou d'une interface de programme. Le consommateur ne gère ni ne contrôle l'infrastructure infonuagique sous-jacente, y compris le réseau, les serveurs, les systèmes d'exploitation, le stockage ou même les capacités d'application individuelles, à l'exception peut-être de paramètres limités de configuration d'application spécifiques à l'utilisateur.
Mise à l'essai	Activité exécutée pour évaluer l'efficacité ou les capacités d'un plan lié à certains objectifs ou critères de mesure. Elle fait habituellement intervenir des exercices conçus pour maintenir l'efficacité des équipes et employés dans l'exécution de leurs tâches et montrer les faiblesses des plans de préparation et d'intervention, de continuité et de reprise.
Vulnérabilité	Mesure dans laquelle une personne, un actif, un processus, une information, une infrastructure ou d'autres ressources sont exposés aux actions ou aux effets d'un risque, d'un événement ou d'une autre occurrence.

Annexe C – Modèles de services infonuagiques



Le modèle de service infonuagique utilisé dans le cadre de cet approvisionnement est le logiciel en tant que service.

Le modèle de prestation en nuage utilisé dans le cadre de cet approvisionnement est public.
Le consommateur est le gouvernement du Canada.
Le fournisseur de services est un fournisseur du SaaS (c.-à-d. le soumissionnaire).

ANNEXE « B » – BASE DE PAIEMENT

Tableau 1 : Besoins initiaux				
Colonne (A)	Colonne (B)	Colonne (C)	Colonne (D)	Colonne (E)
N° d'article	Description	Prix unitaire ferme	Nombre d'utilisateurs aux fins d'évaluation	Prix calculé aux fins d'évaluation
1	Accès des utilisateurs au logiciel-service	\$	3000	1(C) * 1(D)
2	Mise en œuvre, y compris la configuration, la migration des données existantes et le déploiement.	\$	Tarif fixe	2(C)
		Prix ferme		
3	Formation des 20 premiers utilisateurs	\$		3(C)
Prix calculé aux fins d'évaluation				Somme de 1(E) à 3(E)

TABLEAU 2 : Accès pour les utilisateurs supplémentaires (facultatif)				
Colonne (A)	Colonne (B)	Colonne (C)	Colonne (D)	Colonne (E)
N° d'article	Description	PRIX FERME PAR UTILISATEUR	NOMBRE D'UTILISATEURS AUX FINS D'ÉVALUATION	PRIX CALCULÉ AUX FINS D'ÉVALUATION
1. Accès pour les utilisateurs supplémentaires (facultatif)				
1.0	Utilisateurs supplémentaires pour la durée initiale du contrat	\$	500	1,0(C) * 1,0(D)
1.1	Utilisateurs supplémentaires pour la période d'option 1	\$	500	1,1(C) * 1,1(D)
1.2	Utilisateurs supplémentaires pour la période d'option 2	\$	500	1,2(C) * 1,2(D)
1.3	Utilisateurs supplémentaires pour la période d'option 3	\$	500	1,3(C) * 1,3(D)
1.4	Utilisateurs supplémentaires pour la période d'option 4	\$	500	1,4(C) * 1,4(D)
1.5	Utilisateurs supplémentaires pour la période d'option 5	\$	500	1,5(C) * 1,5(D)
1.6	Utilisateurs supplémentaires pour la période d'option 6	\$	500	1,6(C) * 1,6(D)
1.7	Utilisateurs supplémentaires pour la période d'option 7	\$	500	1,7(C) * 1,7(D)
PRIX CALCULÉ AUX FINS D'ÉVALUATION				Somme de 1,0(E) à 1,9(E)

TABLEAU 3 Prestation d'une formation selon les besoins				
Colonne (A)	Colonne (B)	Colonne (C)	Colonne (D)	Colonne (E)
N° d'article	Description	PRIX JOURNALIER FERME	NOMBRE DE JOURS AUX FINS D'ÉVALUATION	PRIX CALCULÉ AUX FINS D'ÉVALUATION
1. De base (utilisateur final)				
1.0	Tarif pour la période initiale du contrat	\$	10	1,0(C) * 1,0(D)
1.1	Tarif pour la période d'option 1	\$	10	1,1(C) * 1,1(D)
1.2	Tarif pour la période d'option 2	\$	10	1,2(C) * 1,2(D)
1.3	Tarif pour la période d'option 3	\$	10	1,3(C) * 1,3(D)
1.4	Tarif pour la période d'option 4	\$	10	1,4(C) * 1,4(D)
1.5	Tarif pour la période d'option 5	\$	10	1,5(C) * 1,5(D)
1.6	Tarif pour la période d'option 6	\$	10	1,6(C) * 1,6(D)
1.7	Tarif pour la période d'option 7	\$	10	1,7(C) * 1,7(D)
2. Formation du formateur				
2.0	Tarif pour la période initiale du contrat	\$	10	2,0(C) * 2,0(D)
2.1	Tarif pour la période d'option 1	\$	10	2,1(C) * 2,1(D)
2.2	Tarif pour la période d'option 2	\$	10	2,2(C) * 2,2(D)
2.3	Tarif pour la période d'option 3	\$	10	2,3(C) * 2,3(D)
2.4	Tarif pour la période d'option 4	\$	10	2,4(C) * 2,4(D)
2.5	Tarif pour la période d'option 5	\$	10	2,5(C) * 2,5(D)
2.6	Tarif pour la période d'option 6	\$	10	2,6(C) * 2,6(D)
2.7	Tarif pour la période d'option 7	\$	10	2,7(C) * 2,7(D)
Prix total aux fins d'évaluation				Somme de 1,0(E) à 1,9(E) + 2,0(E) à 2,9(E)

TABLEAU 4 Prestation de services professionnels selon les besoins				
Colonne (A)	Colonne (B)	Colonne (C)	Colonne (D)	Colonne (E)
N° d'article	Description	PRIX JOURNALIER FERME (par jour)	NOMBRE DE JOURS AUX FINS D'ÉVALUATION	PRIX CALCULÉ AUX FINS D'ÉVALUATION
1.0	Tarif pour la période initiale du contrat	\$	10	1,0(C) * 1,0(D)
1.1	Tarif pour la période d'option 1	\$	10	1,1(C) * 1,1(D)
1.2	Tarif pour la période d'option 2	\$	10	1,2(C) * 1,2(D)
1.3	Tarif pour la période d'option 3	\$	10	1,3(C) * 1,3(D)
1.4	Tarif pour la période d'option 4	\$	10	1,4(C) * 1,4(D)
1.5	Tarif pour la période d'option 5	\$	10	1,5(C) * 1,5(D)
1.6	Tarif pour la période d'option 6	\$	10	1,6(C) * 1,6(D)
1.7	Tarif pour la période d'option 7	\$	10	1,7(C) * 1,7(D)
Prix total aux fins d'évaluation				Somme de 1,0(E) à 1,9(E)
Tableau 5 : Prix total estimatif aux fins de calcul				
Colonne (A)	Colonne (B)	Colonne (C)	Colonne (D)	
N° d'article	Description	Calcul du prix	Prix calculé	
1	Besoins initiaux	Total du tableau 1		\$
2	Accès pour les utilisateurs supplémentaires (facultatif)	Total du tableau 2		\$
3	Prestation d'une formation selon les besoins	Total du tableau 3		\$
4	Prestation de services professionnels selon les besoins	Total du tableau 4		\$
Prix total estimatif aux fins d'évaluation				\$

Solicitation No. – N° de l'invitation
G9292-202457
Client Ref. No. – N° de réf. du client

Amd. No – N° de la modif.
File No. – N° du dossier

Buyer ID – Id de l'acheteur
127 XL
CCC No./N° CCC – FMS No./N° VME

ANNEXE « C » – LISTE DE VÉRIFICATION DES EXIGENCES RELATIVES À LA SÉCURITÉ
(insérer s'il y a lieu)

ANNEXE « D » – GUIDE DE CLASSIFICATION DE SÉCURITÉ

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

N	Rôle ou fonction	Prévision concernant le type de données consulté	Endroit de l'accès aux données (Canada, autre ou les deux)	Filtrage nécessaire	Détails
3.	Tout membre du personnel de l'entrepreneur qui a des rôles privilégiés et un accès logique non restreint à des biens du GC dans les services de l'entrepreneur	<ul style="list-style-type: none">• Toutes les données opérationnelles• Données du GC telles qu'elles sont stockées dans les composantes de calcul, de stockage et de réseau de l'entrepreneur• Données de sécurité, y compris les journaux de vérification des composantes de l'infrastructure de l'entrepreneur• Biens, dont les données et les justificatifs du GC	Les deux	Secret	Cela concerne le personnel de l'entrepreneur qui a des privilèges élevés assortis d'un accès logique sans restriction aux données du GC hébergées dans les centres de données de l'entrepreneur, à tout système sensible, de même qu'aux données sur les incidents de sécurité. Cela comprend l'accès autorisé par l'intermédiaire d'un processus établi comme les demandes juridiques.

N	Rôle ou fonction	Prévision concernant le type de données consulté	Endroit de l'accès aux données (Canada, autre ou les deux)	Filtrage nécessaire	Détails
4.	Tout le personnel de l'entrepreneur ayant un accès physique ou logique aux documents de conception détaillés.	<ul style="list-style-type: none">Documents de conception détaillés de la solution de GSTI, notamment les détails de l'application logique et physique, les architectures de la solution d'infrastructure technologique, les contrôles et l'architecture de sécurité, les détails des diagrammes des composantes, le code source, les détails des cas d'utilisation et des schémas des processus d'activités, les détails de l'application, les flux de données et les modèles de données, les conceptions des bases de données, les interfaces de systèmes, les contrôles internes, les plans des essais et les résultats des essais.	Les deux	Fiabilité	Cela concerne surtout l'accès aux documents relatifs à l'architecture et à la conception détaillée.

N	Rôle ou fonction	Prévision concernant le type de données consulté	Endroit de l'accès aux données (Canada, autre ou les deux)	Filtrage nécessaire	Détails
5.	Personnel du centre des opérations de sécurité (COS) de l'entrepreneur	<ul style="list-style-type: none">Données telles qu'elles sont stockées dans les composantes de calcul, de stockage et de réseau de l'entrepreneurDonnées de sécurité, y compris les journaux de vérification des composantes de l'infrastructure de l'entrepreneur	Les deux	Fiabilité	Il s'agit du personnel du COS de l'entreprise.

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

En plus des rôles susmentionnés, voici les rôles associés aux services relatifs à la transition et à la migration :

Domaine	Rôle	Responsabilités	Accès	Emplacement (autres que pour les réunions)	Exigences en matière de cote de sécurité du personnel (hypothèse de travail)
Gouvernance	Cadre responsable de l'exécution, gestionnaire de programmes ou gestionnaire de projets	Gouvernance ou gestion du projet	Aucun accès aux systèmes physiques (ne touche pas aux claviers) Peut participer à des réunions au cours desquelles les données de configuration des systèmes protégés sont affichées ou discutées Aucun accès aux données des utilisateurs	Sur place, S.O. Accès à distance, Oui	Fiabilité ou l'équivalent
Gestion des services de TI (conseils opérationnels)	Architecte et expert-conseil	Animation d'ateliers, création de documents (plans de service, suivi, etc.)	Aucun accès aux systèmes physiques (ne touche pas aux claviers) Peut participer à des réunions au cours desquelles les données de configuration des systèmes protégés sont affichées ou discutées Aucun accès aux données des utilisateurs	Sur place, S.O. Accès à distance, Oui	Fiabilité ou l'équivalent
Adoption des utilisateurs finaux et gestion du changement	Architecte et expert-conseil	Animation d'ateliers, création de documents, autres activités de gestion du changement requises pour le passage à Office 365	Aucun accès aux systèmes physiques (ne touche pas aux claviers) Peut participer à des réunions au cours desquelles les données de configuration des systèmes protégés sont affichées ou discutées Aucun accès aux données des utilisateurs	Sur place, S.O. Accès à distance, Oui	Aucun accès (suppose qu'il est escorté lorsqu'il se trouve dans les locaux du partenaire)

Intégration à Microsoft Exchange Online	Architecte	Supervision technique du projet, des conseils généraux, des documents et de l'examen des produits livrables	Aucun accès aux systèmes physiques (ne touche pas aux claviers) Accès possible à des documents du gouvernement du Canada de diverses classifications Aucun accès aux données des utilisateurs	Sur place, S.O. Accès à distance, Oui	Fiabilité ou l'équivalent
---	------------	---	---	--	---------------------------

	Expert-conseil en déploiement	<p>Phase de remédiation – Travailler de concert avec les experts en la matière de SPC et du gouvernement du Canada pour remédier à tout problème avec Active Directory local, la configuration en suspens d'Exchange Online local, l'état de préparation du réseau et des clients (bureau).</p> <p>Phase de mise en service – Travailler de concert avec les experts en la matière de SPC et du gouvernement du Canada pour déployer les différents composants (AAD Connect pour la synchronisation, l'établissement de la Fédération pour l'authentification, l'activation de l'accès conditionnel, Azure Information Protection et configuration d'Exchange Online par le locataire)</p>	Accès aux systèmes (location d'Office 365, Active Directory et Exchange versions locales) Accès aux documents du gouvernement du Canada, au besoin, pour aider à la remédiation et à la mise en service Accès potentiel aux données des utilisateurs	Sur place (si SPC l'exige) Accès à distance, Oui	Fiabilité ou équivalent (suppose que SPC gère les environnements indépendamment de la migration des courriels des partenaires)
--	-------------------------------	--	--	---	--

	Expert-conseil en migration	Migration des données de YES vers Exchange Online, y compris la création des projets de migration. Assistance après la migration pour aider les bureaux de service de SPC et des partenaires	Accès aux systèmes (location d'Office 365 en tant qu'administrateur général, Active Directory et Exchange local, YES en tant que direction de l'organisation ou direction des destinataires) Accès ou accès possible aux données (accès complet à la boîte de réception dans YES et Exchange Online) Accès aux documents du gouvernement du Canada, au besoin, pour effectuer les migrations	Sur place (si SPC l'exige) Accès à distance, Oui	Secret ou équivalent
--	-----------------------------	--	--	---	----------------------

ANNEXE « E » – Processus d'intégrité de la chaîne d'approvisionnement

Processus d'intégrité de la chaîne d'approvisionnement

1. Exigences obligatoires

1.1. Les entrepreneurs doivent présenter, avec leur soumission, l'information sur la sécurité de la chaîne d'approvisionnement (ISCA) ci-dessous :

1.2.1 Liste des produits de TI : Les soumissionnaires doivent indiquer les solutions ANS qui pourraient servir à transmettre et à stocker les données du Canada, et qui pourraient être utilisées et installées pour effectuer une partie des travaux ou des services décrits dans le contrat subséquent, en ce qui a trait à chaque solution ANS, en remplissant le formulaire 6 de modèle d'intégrité de la chaîne d'approvisionnement fourni dans la DP, qui comporte les renseignements suivants :

- a) **Nom du FEO :** Inscrivez le nom du fabricant d'équipement d'origine (FEO) du produit commandé.
- b) **Numéro DUNS du FEO :** Inscrivez le numéro DUNS du FEO. Le numéro DUNS (Data Universal Numbering System) est un numéro unique à neuf chiffres attribué à chaque emplacement physique d'une entreprise. Il s'agit d'une norme mondiale utilisée pour déterminer la cote de crédit d'une entreprise. Si l'entreprise n'a pas un numéro DUNS, ou si vous êtes incapable de le trouver, saisissez les renseignements demandés dans la section « C – Renseignements sur les propriétaires ». Les renseignements sur les propriétaires incluent les cinq principaux (en pourcentage) investisseurs et propriétaires de l'entreprise. Le nom des investisseurs et des propriétaires doit être tiré des documents d'investissement ou de propriété de l'entreprise en question.
- c) **Nom du produit :** Inscrivez le nom du FEO du produit.
- d) **Numéro de modèle :** Inscrivez le numéro de modèle ou de version du produit.
- e) **URL du produit :** Inscrivez l'URL de la page du produit du FEO.
- f) **Renseignements sur la vulnérabilité :** Décrivez les cinq derniers problèmes de sécurité signalés pour le produit. Si le FEO a publié l'information sur le site Web CVE, dressez la liste des numéros CVE en les séparant avec des points-virgules (;). Si le FEO n'affiche pas cette information sur le site Web CVE, communiquez directement avec lui pour obtenir des renseignements sur la vulnérabilité en matière de sécurité et transmettez-les au Centre canadien pour la cybersécurité. Si c'est le cas pour un produit particulier, inscrivez « Se reporter aux renseignements ci-joints » dans le champ Renseignements sur la vulnérabilité, et indiquez le ou les noms de fichier dans la colonne des informations supplémentaires qui fournissent les renseignements requis sur la vulnérabilité.

1.2.2 Renseignement sur la propriété : Les entrepreneurs doivent identifier le fabricant d'équipement d'origine (FEO) du ou des produits ou services commandés, ainsi que le nom de tout entrepreneur (c.-à-d. les sous-traitants [particuliers ou entreprises], les sous-traitants des sous-traitants [particuliers ou entreprises] dans la chaîne d'approvisionnement, les revendeurs, distributeurs, sous-traitants ultérieurs, etc.) des produits ou services commandés.

La liste doit indiquer tous les tiers qui pourraient réaliser toute portion des travaux, qu'ils soient sous-traitants d'entrepreneur, ou sous-traitants des sous-traitants d'entrepreneur dans la chaîne d'approvisionnement. Il faut nommer tout sous-traitant d'entrepreneur qui pourrait avoir accès aux données du Canada. Aux fins de la présente exigence, un tiers qui est uniquement un entrepreneur de biens a l'entrepreneur, mais qui n'exécute aucune portion des travaux, n'est pas considéré comme un sous-traitant d'entrepreneur. Les sous-

traitants comprennent notamment les techniciens qui pourraient être déployés ou qui entretiendront la solution d'entrepreneur. Si l'entrepreneur n'entend pas recourir à des sous-traitants pour réaliser une partie des travaux, il devra l'indiquer dans sa réponse.

Les entrepreneurs doivent fournir leurs renseignements sur le formulaire [insérer]. Ils doivent aussi indiquer leur dénomination sociale sur chaque page et inscrire les numéros de page ainsi que le nombre total de pages. Les entrepreneurs doivent en outre insérer une ligne distincte pour chaque sous-traitant ainsi que des lignes supplémentaires, au besoin.

Pour chacune des entités figurant dans la liste, veuillez indiquer l'un ou l'autre de ces éléments :

- a) **Numéro DUNS du FEO** : Inscrivez le numéro DUNS du FEO. Le numéro DUNS (Data Universal Numbering System) est un numéro unique à neuf chiffres attribué à chaque emplacement physique d'une entreprise. Il s'agit d'une norme mondiale utilisée pour déterminer la cote de crédit d'une entreprise. Si l'entreprise n'a pas un numéro DUNS, ou si vous êtes incapable de le trouver, saisissez les renseignements demandés dans la section « C – Renseignements sur les propriétaires ». Les renseignements sur les propriétaires incluent les cinq principaux (en pourcentage) investisseurs et propriétaires de l'entreprise. Le nom des investisseurs et des propriétaires doit être tiré des documents d'investissement ou de propriété de l'entreprise en question.
- b) **Pays et nationalité** : Le pays dont une personne physique a la nationalité principale ou le pays dans lequel est enregistrée une personne morale.
- c) **Lien vers le site Web de l'entreprise** : Pour chaque nom de FEO ou de entrepreneur, de propriétaires, d'investisseurs et de cadres supérieurs énumérés ci-dessus, fournissez une adresse URI ou URL vers l'information qui appuie les allégations énumérées dans chacun des champs.

1.2.3 Diagrammes de réseau : au moins un diagramme de réseau conceptuel montrant, dans leur ensemble, la totalité du réseau proposé pour la prestation des services décrits dans l'ébauche de l'énoncé de travaux (EDT). Les diagrammes de réseau doivent uniquement comprendre les portions du réseau d'entrepreneur (et de ceux de ses sous-traitants) sur lequel des données du Canada seraient transmises dans l'exécution du contrat subséquent. À tout le moins, le diagramme doit illustrer ce qui suit :

- a) Les principaux nœuds suivants servant à la prestation de services dans le cadre du contrat subséquent à la présente demande de soumissions s'ils s'appliquent au rôle d'entrepreneur ou de son sous-traitant;
 - i. Les points de prestation de services;
 - ii. Le réseau de base
 - iii. Les réseaux du sous-traitant (préciser le nom du sous-traitant qui figure dans les **Renseignements sur les propriétaires**);
- b) Les interconnexions entre les nœuds, s'il y a lieu
- c) Toute interconnexion entre les nœuds et Internet;
- d) Pour chaque nœud, un renvoi au produit qui sera déployé dans ce nœud, à l'aide du numéro de ligne du fichier Excel de la liste des produits de TI.

2. Évaluation de l'information sur la sécurité de la chaîne d'approvisionnement (ISCA)

2.1 Le Canada déterminera si, à son avis, l'information sur la sécurité de la chaîne d'approvisionnement donne lieu à la possibilité que la solution d'entrepreneur compromette ou serve à compromettre la sécurité du matériel, des micrologiciels, des logiciels, des systèmes ou des renseignements lui appartenant.

2.2 Au cours de l'évaluation :

- (a) Le Canada peut exiger d'entrepreneur des renseignements supplémentaires qui lui sont nécessaires pour effectuer une évaluation complète de l'information sur la sécurité de la chaîne d'approvisionnement. L'entrepreneur disposera de deux jours ouvrables (ou d'un délai plus long précisé par écrit par l'autorité de la sécurité de la chaîne d'approvisionnement) pour fournir les renseignements nécessaires au Canada. À défaut de respecter ce délai, la réponse sera rejetée.
 - (b) Le Canada peut confier l'évaluation à ses propres ressources ou à des consultants et a le droit, au besoin, de se procurer des renseignements supplémentaires auprès de tiers. Le Canada peut utiliser tout renseignement se trouvant dans la réponse ou provenant d'une autre source et qu'il juge utile pour effectuer une évaluation complète de l'information sur la sécurité de la chaîne d'approvisionnement.
- 2.3 Si le Canada juge que des aspects de l'information sur la sécurité de la chaîne d'approvisionnement, si celle-ci fait partie d'une solution, créent la possibilité que la solution d'entrepreneur puisse compromettre ou servir à compromettre la sécurité du matériel, des micrologiciels, des logiciels, des systèmes ou des renseignements lui appartenant :
- (a) Le Canada écrira (par courriel) à l'entrepreneur pour lui désigner les aspects de l'information sur la sécurité de la chaîne d'approvisionnement qui le préoccupent ou qu'il ne peut pas évaluer (par exemple, des versions à venir de produits ne peuvent être évaluées). Tous les renseignements supplémentaires que le Canada pourrait être en mesure de fournir à l'entrepreneur au sujet de ses préoccupations dépendront de la nature de celles-ci. Pour des raisons de sécurité nationale, il ne sera pas toujours possible pour le Canada de fournir des renseignements supplémentaires à l'entrepreneur. Par conséquent, dans certaines circonstances, l'entrepreneur ne connaîtra pas les raisons sous-jacentes des préoccupations du Canada à l'égard d'un produit, d'un sous-traitant ou d'autres aspects de l'information sur la sécurité de la chaîne d'approvisionnement d'entrepreneur.
 - (b) Après réception de l'avis écrit du Canada, l'entrepreneur pourra présenter de l'information révisée sur la sécurité de la chaîne d'approvisionnement dans un délai de 10 jours civils compté à partir du jour suivant la réception (ou d'un délai plus long précisé par écrit par l'autorité de la sécurité de la chaîne d'approvisionnement).
 - (c) Si l'entrepreneur présente de l'information révisée sur la sécurité de la chaîne d'approvisionnement dans le délai imparti, le Canada procédera à une deuxième évaluation. Si le Canada juge que des aspects de l'information sur la sécurité de la chaîne d'approvisionnement d'entrepreneur peuvent compromettre ou servir à compromettre la sécurité du matériel, des micrologiciels, des logiciels, des systèmes ou des renseignements lui appartenant, il n'offrira pas au répondant d'autre occasion de réviser son information sur la sécurité de la chaîne d'approvisionnement et rejettera sa réponse.
- 2.4 En participant à ce processus, l'entrepreneur reconnaît que la nature de la technologie de l'information est telle que de nouvelles vulnérabilités, y compris celles liées à la sécurité, sont constamment découvertes. En outre, l'entrepreneur reconnaît que l'évaluation de sécurité du Canada ne couvre pas l'évaluation d'une solution proposée. Par conséquent :
- (a) une qualification dans le cadre de la présente DP ne constitue pas une reconnaissance que les produits ou d'autres renseignements inclus dans l'information sur la sécurité de la chaîne d'approvisionnement satisfont aux exigences de la demande de soumissions subséquente et de tout contrat en découlant ou de tout autre instrument pouvant être attribué à la suite d'une demande de soumissions subséquente;

- (b) une qualification dans le cadre de la présente DP ne signifie pas que de l'information sur la sécurité de la chaîne d'approvisionnement identique ou semblable sera évaluée de la même façon pour de futurs besoins;
 - (c) à tout moment au cours du processus de demande de soumissions subséquent, le Canada peut aviser l'entrepreneur que des aspects de l'information sur la sécurité de la chaîne d'approvisionnement suscitent des préoccupations en matière de sécurité. À ce stade, le Canada avisera le répondant et offrira à l'entrepreneur l'occasion de réviser son information sur la sécurité de la chaîne d'approvisionnement selon le processus décrit ci-dessus.
 - (d) au cours de l'exécution d'un contrat de sous-traitance subséquent, si le Canada est préoccupé par des produits, conceptions ou sous-traitants compris initialement dans l'information sur la sécurité de la chaîne d'approvisionnement, il gèrera ces préoccupations conformément aux modalités du contrat.
- 2.5 Tous les entrepreneurs seront avisés par écrit s'ils se sont ou non qualifiés dans le cadre de la DP pour passer à l'étape suivante du processus d'approvisionnement.
- 2.6 Les entrepreneurs retenus dans le cadre de la DP devront, dans leur réponse à une demande de soumissions subséquente, proposer une solution conforme à la version définitive de l'information sur la sécurité de la chaîne d'approvisionnement qu'ils ont transmise avec leur réponse à la présente DP (sous réserve de révision conformément au paragraphe ci-dessous seulement). Sauf conformément au paragraphe ci-dessous, aucun produit ou sous-traitant autre ou supplémentaire ne peut être proposé dans la solution d'entrepreneur. Il s'agit d'une exigence obligatoire de ce processus de demande de soumissions. La solution proposée dans toute demande de soumissions subséquente ne doit pas contenir tous les produits inclus dans l'information sur la sécurité de la chaîne d'approvisionnement.
- 2.7 Une fois qu'un entrepreneur a été retenu dans le cadre de la présente DP, aucune modification ne peut être apportée à l'information sur la sécurité de la chaîne d'approvisionnement, sauf dans des circonstances exceptionnelles déterminées par le Canada. Comme il n'est pas possible de prévoir toutes les circonstances exceptionnelles, le Canada, pour chacun des cas qui se présentent, déterminera si des modifications sont permises et définira le processus régissant ces modifications.

ANNEXE « F » – Information sur la sécurité de la chaîne d'approvisionnement

Formulaire de soumission des fournisseurs



PARTIE A – RENSEIGNEMENTS SUR LE SOUMISSIONNAIRE	
Nom de la soumission :	
Date de soumission :	
Numéro de la soumission :	
Nom du soumissionnaire :	
Numéro DUNS du soumissionnaire :	



B – Liste des produits

Exemple de liste
des produits
informatiques

Article	Nom du FEO	Numéro DUNS du FEO	Nom du produit	Modèle/version	URL du produit	Renseignements sur la vulnérabilité	Nom du fournisseur	Numéro DUNS du fournisseur	URL du fournisseur	Info supplémentaires
1										
2										
3										
4										
5										
6										
7										
8										
9										
10										
11										
12										

8					
9					
10					
11					
12					
13					
14					
15					

D – Aide

Champ	Guide	Remarques
Page couverture du formulaire 2 de l'ISCA		
NOM DE L'AGENT D'APPROVISIONNEMENT	"Si ce champ ne s'applique pas, laissez-le vide. Autrement, inscrivez le nom associé à l'approvisionnement de produits multiples (p. ex. WTD Print, Projet Telesto)."	
Date de présentation :	AAAA-MM-JJ	
N° DE LA DEMANDE DE SOUMISSIONS :	"Si ce champ ne s'applique pas, laissez-le vide. Autrement, inscrivez le numéro de la soumission liée à l'approvisionnement de produits multiples."	

NOM DU SOUSSIONNAIRE	"Si ce champ ne s'applique pas, laissez-le vide. Inscrivez le nom de l'organisation qui se charge de présenter la soumission."	
NUMÉRO DUNS DU SOUSSIONNAIRE	"Si ce champ ne s'applique pas, laissez-le vide. Inscrivez le numéro DUNS de l'organisation qui se charge de présenter la soumission. Si l'organisation n'a pas de numéro DUNS ou que vous n'arrivez pas à le trouver, veuillez remplir la partie C : « Information sur la propriété ». L'information sur la propriété concerne les 5 principaux propriétaires et investisseurs de l'entreprise, en fonction du pourcentage. Le nom des investisseurs et propriétaires doit correspondre à celui qui paraît dans les documents d'investissement ou de propriété de l'entreprise en question."	
LISTE DES PRODUITS DE TI		
Nom du FEO	Inscrivez le nom du fabricant d'équipement d'origine (FEO) du produit commandé.	Seuls les produits admissibles à l'évaluation de l'intégrité de la chaîne d'approvisionnement doivent paraître dans cette liste. Ne tenez pas compte des câbles d'alimentation, des panneaux de remplissage de bâtis, des coûts liés à la garantie, des frais d'expédition et d'autres éléments non liés aux technologies de l'information et des communications (TIC). Si ce type de produit est inscrit dans le formulaire, ce dernier vous sera renvoyé et aucune évaluation ne sera réalisée. Tout produit inscrit dans le formulaire doit respecter la définition de « produit », c'est-à-dire « tout matériel qui fonctionne dans la couche de liaison de données du modèle OSI [Open Systems Interconnection] (couche 2) ou supérieure, tout logiciel et tout appareil technologique en milieu de travail ».
Numéro DUNS du FEO	Entrez le numéro DUNS du FEO. Le numéro DUNS (Data Universal Numbering System) est un numéro unique à neuf chiffres attribué à chaque emplacement physique d'une entreprise. Il s'agit d'une norme mondiale utilisée pour déterminer la cote de crédit d'une entreprise. Si l'entreprise n'a pas de numéro DUNS, ou si vous êtes incapable de le trouver, saisissez les renseignements demandés dans la section « C – Informations sur la propriété ». Les renseignements sur les propriétaires incluent les cinq principaux (en pourcentage) investisseurs et propriétaires de l'entreprise. Le nom des investisseurs et des propriétaires doit être tiré des documents d'investissement ou de propriété de l'entreprise en question.	
Nom du produit	Entrez le nom du FEO du produit.	
Numéro de modèle	Entrez le numéro de modèle ou de version du produit.	
URL du produit	Inscrivez l'adresse URL de la page Web du FEO où se trouve le produit.	

Renseignements sur la vulnérabilité	<p>"Inscrivez l'information sur les 5 derniers problèmes de sécurité qui ont touché le produit. Si le FEO affiche cette information sur le site Web des vulnérabilités et expositions courantes (CVE), inscrivez les numéros CVE et séparez-les par un point-virgule (;).</p> <p>Si le FEO n'affiche pas cette information sur le site Web des CVE, vous devrez communiquer directement avec lui pour obtenir les renseignements sur les vulnérabilités informatiques, puis les transmettre au Centre canadien pour la cybersécurité. Si cette situation s'applique à un produit particulier, inscrivez « voir l'information ci-jointe » dans le ou les champs pertinents."</p>	
Nom du fournisseur	<p>"Inscrivez le nom du fournisseur du produit commandé (c'est-à-dire les sous-traitants, les revendeurs, les distributeurs, les entités chargées du traitement des données, etc.). Il s'agit de toute entité commerciale appelée à fournir des produits ou services dans le but de remplir les exigences de la soumission.</p> <p>Dans le cas d'un arrangement en matière d'approvisionnement relatif à l'infrastructure matérielle (AAIM), d'une offre à commandes principale et nationale (OCPN), ou d'autres listes, le champ peut rester vide."</p>	

Numéro DUNS du fournisseur	<p>"Inscrivez le numéro DUNS du fournisseur. Le numéro Data Universal Numbering System (DUNS) est un identifiant numérique unique de neuf chiffres attribué à chaque emplacement physique d'une entreprise. Il s'agit d'une norme internationale qui sert à établir la cote de crédit d'une entreprise. Si l'organisation n'a pas de numéro DUNS ou que vous n'arrivez pas à le trouver, veuillez remplir la « partie C - Information sur la propriété ». L'information sur la propriété concerne les 5 principaux propriétaires et investisseurs de l'entreprise, en fonction du pourcentage. Le nom des investisseurs et propriétaires doit correspondre à celui qui paraît dans les documents d'investissement ou de propriété de l'entreprise en question.</p> <p>Dans le cas d'un AAIM, d'une OCPN, ou d'autres listes, le champ peut rester vide."</p>	
URL du fournisseur	<p>"Inscrivez l'adresse URL de la page Web du fournisseur où se trouve le produit.</p> <p>Dans le cas d'un AAIM, d'une OCPN, ou d'autres listes, le champ peut rester vide."</p>	
INFORMATION SUR LA PROPRIÉTÉ		
Nom du fournisseur ou du FEO	Inscrivez le nom du fabricant d'équipement d'origine (FEO) du produit commandé ou le nom du fournisseur (c'est-à-dire les sous-traitants, les revendeurs, les distributeurs, les entités chargées du traitement des données, etc.) du produit ou service commandé.	<p>"Vous devez remplir les champs de la partie C : « Information sur la propriété » uniquement si vous n'êtes pas en mesure de fournir le numéro DUNS du FEO ou du fournisseur.</p> <p>Chaque ligne et chaque cellule du tableau doit comporter un seul élément d'information."</p>
Propriété	Il s'agit des 5 principaux propriétaires du FEO ou du fournisseur, en fonction du pourcentage. Le nom des propriétaires doit correspondre à celui qui paraît dans les documents de propriété de l'entreprise en question.	
Investisseurs	Il s'agit des 5 principaux investisseurs du FEO ou du fournisseur, en fonction du pourcentage. Le nom des investisseurs doit correspondre à	

Sollicitation No. – N° de l'invitation
G9292-202457
Client Ref. No. – N° de réf. du client

Amd. No. – N° de la modif.
File No. – N° du dossier

Buyer ID – Id de l'acheteur
127 XL
CCC No./N° CCC – FMS No./N° VME

	celui qui paraît dans les documents d'investissement de l'entreprise en question.	
Cadres supérieurs	Inscrivez le nom des membres de la direction et du conseil d'administration de l'entreprise en question.	

Pays ou nationalité	Il s'agit du pays de nationalité de la personne ou du pays où l'entité commerciale est enregistrée. Pour chaque FEO, fournisseur, propriétaire, investisseur ou membre de la direction inscrit dans le tableau, donnez l'adresse URI / URL vers l'information à l'appui des renseignements fournis dans chacun des champs.
Lien vers le site Web de l'entreprise	

E – Exemple de liste des produits de TI

Arti cle	Nom du FEO	Numéro DUNS du FEO	Nom du produit	Modèle /versio n	URL du produit	Renseignements sur les vulnérabilités	Nom du fournisseur	Numéro DUNS du fournisseu r	URL du fournisseur	INFORMATION ADDITIONNELLE
1	Cie. ABC	137660665	1941	K9	Ajouter URL ici	CVE-2018-XXXXX; CVE-2018-YYYYY; CVE-2018-XXXXX; CVE-2017- WWWWW				Exemple d'un AAIM
2	Cie. ABC	137660665	1941	K9	Ajouter URL ici	CVE-2018-XXXXX; CVE-2018-YYYYY; CVE-2018-XXXXX; CVE-2017- WWWWW	MatérielLoyal	4567891234	https://www.lhinc.ca	Exemple d'arrangement autre qu'un AAIM ou de l'approvisionnement d'un seul produit

F – Exemple d’informations sur la propriété

Nom du fournisseur ou du FEO	Propriété	Investisseurs	Cadres supérieurs	Pays ou nationalité	Lien vers le site Web de l'entreprise
Logiciel newkid	M. A (60 %)			Canada	newkid.com/profiles/ma
Logiciel newkid	M ^{me} B (30 %)			France	newkid.com/profiles/mmeb
Logiciel newkid	M. C (10 %)			États-Unis	newkid.com/profiles/mc
Logiciel newkid		Entreprise A (10 %)		États-Unis	newkid.com/relations_investisseurs/publications
Logiciel newkid		Entreprise B (9 %)		Chine	newkid.com/relations_investisseurs/publications
Logiciel newkid		Entreprise C (8 %)		Corée du Sud	newkid.com/relations_investisseurs/publications
Logiciel newkid		Entreprise D (5 %)		Canada	newkid.com/relations_investisseurs/publications
Logiciel newkid		Entreprise E (5 %)		Espagne	newkid.com/relations_investisseurs/publications
Logiciel newkid			M. A	Canada	newkid.com/profiles/ma
Logiciel newkid			M ^{me} B	France	newkid.com/profiles/mmeb
Logiciel newkid			M. Q	Portugal	newkid.com/profiles/mq

Annexe « G » – Entente de non-divulgence de SPAC relatif à l'intégrité de la chaîne d'approvisionnement

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

Entente de non-divulgence

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

1. L'entrepreneur accepte d'assurer la confidentialité de toute information qu'il reçoit du Canada au sujet de l'évaluation qu'a faite ce dernier de l'information sur la sécurité de la chaîne d'approvisionnement fournie par l'entrepreneur (l'« **information sensible** »), y compris, sans toutefois s'y limiter, les aspects de l'information sur la sécurité de la chaîne d'approvisionnement qui soulèvent des préoccupations, et les raisons qui ont mené aux interrogations du Canada à cet égard.
2. L'information sensible comprend, mais pas exclusivement, les documents, instructions, directives, données, éléments matériels, avis ou autres, qu'ils aient été reçus verbalement, sous forme imprimée ou d'une autre façon ou qu'ils soient ou non considérés comme classifiés, exclusifs ou sensibles.
3. L'entrepreneur convient de ne pas reproduire, copier, divulguer, publier ou communiquer, en tout ou en partie, de quelque façon que ce soit, de l'information sensible à une autre personne qu'un employé d'entrepreneur détenant une habilitation de sécurité correspondant à la sensibilité de l'information consultée, sans le consentement écrit préalable de l'autorité de la sécurité de la chaîne d'approvisionnement. L'entrepreneur accepte d'aviser immédiatement l'autorité de la sécurité de la chaîne d'approvisionnement dès qu'une personne, autre que celles autorisées en vertu du présent article, accède à de l'information sensible.
4. Toute l'information sensible demeure la propriété du Canada et doit être retournée à l'autorité de sécurité de la chaîne d'approvisionnement ou détruite à la demande de cette dernière dans les 30 jours suivant cette demande.
5. L'entrepreneur, est conscient qu'un manquement à cette entente de non-divulgence peut entraîner sa disqualification à l'étape de l'arrangement en matière d'approvisionnement (AMA), ou une résiliation immédiate du contrat subséquent. L'entrepreneur reconnaît également que toute violation de cette entente de non-divulgence peut entraîner un examen de sa cote de sécurité ainsi qu'un examen de son statut en tant que soumissionnaire admissible pour d'autres besoins.
6. La présente entente de non-divulgence demeure en vigueur indéfiniment.

ANNEXE « H » – PROGRAMME D'ÉVALUATION DE LA SÉCURITÉ DES TI DES LOGICIELS-SERVICES : PROCESSUS D'INTÉGRATION

1. Présenter une soumission au Programme d'évaluation de la sécurité des TI des logiciels-services

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

2. Clé PGP

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

3. Personnes-ressources et assistance

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

Centre d'appel du CCC

contact@cyber.gc.ca

613-949-7048 ou 1-833-CYBER-88

ANNEXE « I » – Accords sur les niveaux de service (ANS) du ANS

Uniquement les modalités de l'ANS, détaillées à la section 1 du paragraphe 3.3 : La présentation technique, (c)(iv), relative aux niveaux de service et à la prestation des services fera partie du Contrat. En présentant une soumission, l'entrepreneur reconnaît et convient que toutes les modalités contenues à l'annexe G – Accords sur les niveaux de service de la solution ANS qui visent à interpréter le contrat, qui sont le même sujet ou un sujet semblable, ou qui sont liées aux modalités contenues dans les clauses du contrat, sont réputées être annulées et inopérantes. De même, toute clause contenue à l'annexe G – Accords sur les niveaux de service du ANS qui comprend des renseignements sur les prix,

comme (sans s'y limiter) ceux qui tentent d'imposer des conditions financières, des modalités de prix ou des pénalités de conformité, sera réputée être annulée et inopérante.

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

**ANNEXE « J » de la PARTIE 5 DE LA DEMANDE DE SOUMISSIONS
PROGRAMME DE CONTRATS FÉDÉRAUX POUR L'ÉQUITÉ EN MATIÈRE D'EMPLOI –
ATTESTATION**

(insérer s'il y a lieu)

En présentant les renseignements suivants à l'autorité contractante, j'atteste, en tant que soumissionnaire, que les renseignements fournis sont exacts à la date indiquée ci-après. Les attestations fournies au gouvernement du Canada peuvent faire l'objet d'une vérification à tout moment. Je comprends que le Canada déclarera une soumission non recevable, ou un manquement de la part d'entrepreneur, s'il est établi qu'une attestation est fausse, que ce soit pendant la période d'évaluation des soumissions ou pendant la durée du contrat. Le Canada aura le droit de demander des renseignements supplémentaires pour vérifier les attestations du soumissionnaire. Le non-respect de toute demande ou exigence imposée par le Canada peut rendre la soumission irrecevable ou constituer un manquement au contrat.

Pour en savoir plus sur le Programme des contrats fédéraux pour l'équité en matière d'emploi, consultez le site Web [Emploi et Développement social Canada – Programme du travail](#).

Date : _____ (AAAA-MM-JJ) (si aucune date n'est indiquée, la date de clôture des soumissions sera utilisée.)

Remplissez les sections A et B.

A. Cochez l'une des déclarations suivantes :

- ☐ A1. Le soumissionnaire atteste qu'il n'a aucun effectif au Canada.
- ☐ A2. Le soumissionnaire atteste qu'il est un employeur du secteur public.
- ☐ A3. Le soumissionnaire atteste qu'il est un employeur assujetti à la législation fédérale, en vertu de la Loi sur l'équité en matière d'emploi.
- ☐ A4. Le soumissionnaire atteste qu'il a un effectif combiné de moins de 100 employés permanents à temps plein ou permanents à temps partiel au Canada.
- A5. Le soumissionnaire a un effectif combiné de 100 employés ou plus au Canada.
- ☐ A5.1. Le soumissionnaire atteste qu'il a signé un Accord pour la mise en œuvre de l'équité en matière d'emploi valide et en vigueur avec EDSC – Programme du travail.
- OU**
- ☐ A5.2. Le soumissionnaire atteste qu'il a présenté le formulaire d'Accord pour la mise en œuvre de l'équité en matière d'emploi (LAB1168) au Programme du travail d'EDSC. Comme il s'agit d'une condition préalable à l'attribution du contrat, remplissez le formulaire d'Accord pour la mise en œuvre de l'équité en matière d'emploi (LAB1168), signez-le, puis transmettez-le aux responsables du Programme du travail d'EDSC.

B. Cochez une des déclarations suivantes :

- ☐ B1. Le soumissionnaire n'est pas une coentreprise.

OU

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

**ANNEXE « K » FORMULAIRE TPSGC-PWGSC 572 – AUTORISATION DE TÂCHE
FORMULAIRE D'AUTORISATION DE TÂCHES
CONTRAT DU SAGU
FORMULAIRE D'AUTORISATION DE TÂCHES (AT)
SUR DEMANDE**

Entrepreneur :		Numéro du contrat	
Code financier :		Codage financier de TPS :	
Autorisation de tâches n° :		Date :	
1.0 DESCRIPTION DES TÂCHES OU DES TRAVAUX À EXÉCUTER			
2.0 PÉRIODE DES SERVICES			
Du :		Au :	
3.0 SERVICES À FOURNIR À : (EMPLACEMENT/ADRESSE)			
4.0 RESPONSABLES			
Chargé de projet :		Centre de responsabilité :	
5.0 COÛT			
Catégorie et niveau de personnel/catégorie de cours	Tarif quotidien/tarif par cours	Nombre de jours pour exécuter les tâches/travaux	Total
	\$		\$
	\$		\$
	\$		\$
	\$		\$
	\$		\$
		PRIX ESTIMATIF	\$
		TPS/TVH	\$
		TOTAL	\$
Frais de déplacement et de subsistance : Les frais de déplacement et de subsistance seront facturés directement selon le principe des frais remboursables. Toutes les dépenses doivent être engagées conformément aux lignes directrices du Conseil du		PRIX ESTIMATIF	\$

<p>Trésor en vigueur à ce moment. Les factures associées à des frais de déplacement et de subsistance présentées par les employés d'entrepreneur doivent être accompagnées de pièces justificatives (reçus) et seront remboursées conformément à la politique et aux lignes directrices du Conseil du Trésor sur les voyages, en vigueur au moment des déplacements, au coût réel, sans provision pour la marge bénéficiaire. Les frais de transport aérien ne dépasseront pas les tarifs de classe économique.</p>		
	<p>TPS/TVH</p>	<p>0 \$</p>
	<p>TOTAL</p>	<p>0 \$</p>
	<p>TOTAL GÉNÉRAL</p>	<p>\$</p>
<p>L'entrepreneur est tenu de vendre à Sa Majesté la Reine du chef du Canada, conformément aux modalités établies ou mentionnées dans la présente ou ci-jointes, les services énumérés dans la présente ou sur les feuilles jointes, au prix établi.</p>		

ANNEXE « L » Formulaire d'autorisation de l'éditeur de logiciels-services

Annexe L - Formulaire d'autorisation de l'éditeur de logiciels-services

(à remplir lorsque le fournisseur n'est pas l'éditeur de logiciels)

Ce formulaire vise à confirmer que l'éditeur de logiciels-services nommé ci-dessous comprend et atteste que [inscrire le nom du revendeur] a présenté une soumission en réponse à la demande d'arrangement en matière d'approvisionnement émise par SPAC le [inscrire la date _____], numéro de référence _____. L'éditeur de logiciels confirme par la présente que

- (i) le fournisseur nommé ci-dessous est autorisé à fournir les Solutions de logiciels-services décrites ci-dessous ou jointes aux présentes, par l'entremise de son AMA;
- (ii) l'éditeur de logiciels-services accepte d'accorder toutes les licences qui doivent être acquises dans le cadre de l'AMA, conformément aux modalités du contrat subséquent établies dans l'AMA.

L'éditeur de logiciels-services reconnaît que le fournisseur a proposé à l'État les logiciels exclusifs de l'entreprise suivants en réponse à la DAMA.

[Inscrire tous les logiciels exclusifs faisant l'objet d'une licence qui sont proposés par le fournisseur.]

(Les fournisseurs doivent ajouter ou supprimer des lignes au besoin.)

Nom de l'éditeur de logiciels-services

Signature du fondé de signature de l'éditeur de logiciels-services

Nom en caractères d'imprimerie du fondé de signature de l'éditeur de logiciels-services

Titre en caractères d'imprimerie du fondé de signature de l'éditeur de logiciels-services

Adresse du fondé de signature de l'éditeur de logiciels-services

N° de téléphone du fondé de signature de l'éditeur de Logiciels-services

N° de télécopieur du fondé de signature de l'éditeur de Logiciels

Date de signature

Nom du fournisseur