National Defence | Défense nationale

National Defence Headquarters
Ottawa, Ontario
K1A 0K2

Quartier général de la Défense nationale
Ottawa (Ontario)
K1A 0K2

REQUEST FOR PROPOSAL / DEMANDE DE PROPOSITION

RETURN BIDS TO / RETOURNER LES SOUMISSIONS À:

Direction des contrats de service 3 (D C Svc 3)
Attention: Lana Ibrahim, DC Svcs 3-4-2
Par courriel : Lana.Ibrahim@forces.gc.ca

Proposal To: National Defence 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 and services listed herein and on any attached sheets at the price(s) set out therefore.

Proposition à: Défense nationale 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 et services énumérés ici et sur toute feuille ci-annexée, au(x) prix indique(s).

Comments – Commentaires

THIS DOCUMENT CONTAINS A SECURITY REQUIREMENT
CE DOCUMENT CONTIENT UNE EXIGENCE DE SÉCURITÉ.

Solicitation Closes / L'invitation prend fin:

At / à:

14:00 Heure normale de l'Est (HNE)

On / le:

26 Janvier 2023

Title / Titre	**Solicitation No. / N° de l'invitation**
Système de surveillance de l'environnement	W6369-22-A009

Date of Solicitation / Date de l'invitation
14 Décembre 2022

Address Enquiries to / Adresser toutes questions à:

Lana Ibrahim, DC Svcs 3-4-2
Lana.Ibrahim@forces.gc.ca

Telephone No. / N° de téléphone	**FAX No. / N° de fax**

Destination

Quartier général de la Défense nationale
Dépôt central de matériel médical
105, chemin Montgomery, bâtiment BB-104-A
Petawawa (Ontario)
K8H 2X3

Instructions: Municipal taxes are not applicable. Unless otherwise specified herein all prices quoted must include all applicable Canadian customs duties, GST/HST, excise taxes and are to be delivered Delivery Duty Paid including all delivery charges to destination(s) as indicated. The amount of the Goods and Services Tax/Harmonized Sales Tax is to be shown as a separate item.

Instructions : Les taxes municipales ne s'appliquent pas. Sauf indication contraire, les prix indiqués doivent comprendre les droits de douane canadiens, la TPS/TVH et la taxe d'accise. Les biens doivent être livrés « rendu droits acquittés », tous frais de livraison compris, à la ou aux destinations indiquées. Le montant de la taxe sur les produits et services/taxe de vente harmonisée doit être indiqué séparément.

Delivery Required / Livraison exigée	**Delivery Offered / Livraison proposée**

Vendor Name and Address / Raison sociale et adresse du fournisseur

Name and title of person authorized to sign on behalf of vendor (type or print) / Nom et titre de la personne autorisée à signer au nom du fournisseur (caractère d'imprimerie)

Name – Nom _____ Title – Titre _____

Signature _____ Date _____

National Defence | Défense nationale

National Defence Headquarters
Ottawa, Ontario
K1A 0K2

Quartier général de la Défense nationale
Ottawa (Ontario)
K1A 0K2

TABLE DES MATIÈRES

PARTIE 1 – RENSEIGNEMENTS GÉNÉRAUX

1.1 Introduction

A. La demande de soumissions contient sept parties, ainsi que des pièces jointes et des annexes, et elle est divisée comme suit :

Partie 1 Renseignements généraux : renferme une description générale du besoin;

Partie 2 Instructions à l'intention des soumissionnaires : renferme les instructions, clauses et conditions relatives à la demande de soumissions;

Partie 3 Instructions pour la préparation des soumissions : donne aux soumissionnaires les instructions pour préparer leur soumission;

Partie 4 Procédures d'évaluation et méthode de sélection : décrit la façon selon laquelle se déroulera l'évaluation et présente les critères d'évaluation auxquels on doit répondre dans la soumission, ainsi que la méthode de sélection;

Partie 5 Attestations et renseignements supplémentaires : comprend les attestations et les renseignements supplémentaires à fournir;

Partie 6 Exigences relatives à la sécurité, exigences financières et autres exigences : comprend des exigences particulières auxquelles les soumissionnaires doivent répondre; et

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

B. Les pièces jointes comprennent le Barème de prix, les Critères techniques attestation et toute autre pièces jointes.

C. Les annexes comprennent l'Énoncé des besoins, la Base de paiement, la Liste de vérification des exigences relatives à la sécurité, et toute autre annexe.

1.2 Sommaire

A. Le ministère de la Défense nationale (MDN) a besoin d'un système de surveillance de l'environnement doté d'enregistreurs de données et d'alarmes pour contrôler de façon continue et à distance la température des réfrigérateurs entre 2 et 8 °C et des congélateurs à -20 °C et à 80 °C déployés pour l'entreposage de vaccins contre la COVID-19. Les biens seront livrés au dépôt central de matériel médical du 105, chemin Montgomery, à Ottawa, en Ontario.

La période initiale du contrat s'étendra de la date d'attribution du contrat au 31 mars 2024. Tous les produits livrables doivent être reçus au plus tard le 30 août 2023 pour la période initiale du contrat. Les biens et services optionnels requis sur demande doivent être livrés avant le 31 mars 2027.

B. Ce besoin comporte des exigences relatives à la sécurité. Pour de plus amples renseignements, consulter la Partie 6, Exigences relatives à la sécurité, exigences financières et autres exigences, et la Partie 7, Clauses du contrat subséquent. Pour de plus amples renseignements sur les enquêtes de sécurité sur le personnel et les organismes, les soumissionnaires devraient consulter le site Web du Programme de sécurité industrielle (PSI) de Travaux publics et Services gouvernementaux Canada (http://ssi-iss.tpsgc-pwgsc.gc.ca/index-fra.html).

C. Ce besoin est assujetti aux dispositions de l'Accord de libre-échange Canada-Chili, de l'Accord de Partenariat Transpacifique global et progressiste (PTPGP), de l'Accord de libre-échange Canada Colombie, de Canada et l'Union européenne Accord économique et commercial global (AECG), de l'Accord de libre-échange Canada Honduras, de l'Accord de libre-échange Canada-Corée, de l'Accord libre-échange entre le Canada et le Panama, de l'Accord de libre-échange Canada-Pérou, de l'Accord de libre-échange Canada-Ukraine, de l'Accord de continuité commerciale Canada–Royaume-Uni (ACC Canada-Royaume-Uni) - de Accord de continuité commerciale, de l'Accord libre-échange entre de l'Accord sur les marchés publics de l'Organisation mondiale du commerce (AMP-OMC), et de l'Accord de libre-échange canadien (ALEC).

1.3 Compte rendu

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

PARTIE 2 – INSTRUCTIONS À L'INTENTION DES SOUMISSIONNAIRES

2.1 Instructions, clauses et conditions uniformisées

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

B. 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.

C. Le document 2003 (2022-03-29), Instructions uniformisées - biens ou services - besoins concurrentiels, est incorporé par renvoi dans la demande de soumissions et en fait partie intégrante, avec les modifications suivantes :

(i) La section 02, Numéro d'entreprise - approvisionnement, est supprimée dans sa totalité;

(ii) La section 05, Présentation des soumissions, sous-alinéa 2., paragraphe d., est supprimé en entier et remplacé comme suit :

d. de faire parvenir sa soumission uniquement au Ministère de la Défense nationale (MDN) tel qu'indiqué à la page 1 de la demande de soumissions ou à l'adresse indiquée dans la demande de soumissions.

(iii) La section 05, Présentation des soumissions, sous-alinéa 2., paragraphe e., est supprimé en entier et remplacé comme suit :

e. s'assurer que le nom du soumissionnaire, l'adresse de retour, le numéro de la soumission, ainsi que la date et l'heure de la clôture de la soumission apparaissent clairement sur la soumission; et

(iv) La section 05, Présentation des soumissions, sous-alinéa 3, est supprimé.

(v) La section 05, Présentation des soumissions, sous-alinéa 4, est modifiée comme suit :

Supprimer : 60 jours
Insérer : 180 jours

(vi) La section 06, Soumissions déposées en retard, est supprimée en entier;

(vii) La section 07, Soumissions retardées, est supprimé en entier et remplacé comme suit :

07 Soumissions retardées

1. Il incombe au soumissionnaire de s'assurer que l'autorité contractante a reçu la soumission complète. Les soumissions qui sont reçues en retard à cause d'une erreur d'acheminement ou de tout autre problème de livraison ne seront pas acceptées.

(viii) La section 08, Transmission par télécopieur, est supprimée en entier; et

(ix) La section 20, Autres renseignements, est supprimée en entier.

2.2 Présentation des soumissions

A. Les soumissions doivent être présentées uniquement au ministère de la Défense nationale (MDN)) au plus tard à la date, à l'heure et à l'endroit indiqués à la page 1 de la demande de soumissions.

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

2.2.1 Présentation des soumissions par voie électronique

A. **Le système de messagerie électronique ou les pare-feu du Canada peuvent refuser les courriels individuels excédant cinq (5) mégaoctets ou comprenant certains scripts, mises en forme, macros ou hyperliens intégrés, et ce, sans qu'un avis soit envoyé au soumissionnaire ou à l'autorité contractante.** Les soumissions plus volumineuses peuvent être envoyées en plusieurs courriels. Le Canada accusera réception des documents. Il incombe au soumissionnaire de s'assurer que sa soumission a été reçue en entier. Le soumissionnaire ne devrait pas supposer que tous ses documents ont été reçus, sauf si le Canada accuse réception de chaque document. Afin de réduire les risques de problèmes techniques, le soumissionnaire doit prévoir suffisamment de temps avant la date et l'heure de clôture pour l'accusé de réception de ses documents. Les documents **soumis** après la date et l'heure de clôture seront rejetés.

2.3 Demandes de renseignements - en période de soumission

A. Toutes les demandes de renseignements doivent être présentées par écrit à l'autorité contractante au moins dix (10) jours civils avant la date de clôture des soumissions. Pour ce qui est des demandes de renseignements reçues après ce délai, il est possible qu'on ne puisse pas y répondre.

B. Les soumissionnaires devraient citer le plus fidèlement possible le numéro de l'article de la demande de soumissions auquel se rapporte la question et prendre soin d'énoncer chaque question de manière suffisamment détaillée pour que le Canada puisse y répondre avec exactitude. Les demandes de renseignements techniques qui ont un caractère exclusif doivent porter clairement la mention « exclusif » vis-à-vis de chaque article pertinent. Les éléments portant la mention « exclusif » feront l'objet d'une discrétion absolue, sauf dans les cas où le Canada considère que la demande de renseignements n'a pas un caractère exclusif. Dans ce cas, le Canada peut réviser les questions ou peut demander au soumissionnaire de le faire, afin d'en éliminer le caractère exclusif, et permettre la transmission des réponses à tous les soumissionnaires. Le Canada peut ne pas répondre aux demandes de renseignements dont la formulation ne permet pas de les diffuser à tous les soumissionnaires.

2.4 Lois applicables

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

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

2.5 Processus de contestation des offres et mécanismes de recours

A. Les fournisseurs potentiels ont accès à plusieurs mécanismes pour contester des aspects du processus d'approvisionnement jusqu'à l'attribution du marché, inclusivement.

B. Le Canada invite les fournisseurs à porter d'abord leurs préoccupations à l'attention de l'autorité contractante. Le site Web du Canada Achats et ventes, sous le titre « Processus de contestation des soumissions et mécanismes de recours », fournit de l'information sur les organismes de traitement des plaintes possibles, notamment :

- Bureau de l'ombudsman de l'approvisionnement (BOA)
- Tribunal canadien du commerce extérieur (TCCE)

C. Les fournisseurs devraient savoir que des **délais stricts** sont fixés pour le dépôt des plaintes et qu'ils varient en fonction de l'organisation concernée. Les fournisseurs devraient donc agir rapidement s'ils souhaitent contester un aspect du processus d'approvisionnement.

PARTIE 3 – INSTRUCTIONS POUR LA PRÉPARATION DES SOUMISSIONS

3.1 Instructions pour la préparation des soumissions

A. Le Canada demande que les soumissionnaires fournissent leur soumission en sections distinctes, comme suit :

Section I: Soumission technique : une (1) copie de format PDF envoyé par courrier électronique;

Section II: Soumission financière : une (1) copie de format PDF envoyé par courrier électronique;

Section III: Attestations : une (1) copie de format PDF envoyé par courrier électronique; et

Section IV: Renseignements supplémentaires : une (1) copie de format PDF envoyé par courrier électronique;

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

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

(i) utiliser du papier de 8,5 po x 11 po (216 mm x 279 mm); et

(ii) utiliser un système de numérotation correspondant à celui de la demande de soumissions.

3.2 Section I : Soumission technique

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

B. La soumission technique devrait traiter clairement et de manière suffisamment approfondie des points faisant l'objet des critères d'évaluation en fonction desquels la soumission sera évaluée. Il ne suffit pas de reprendre simplement les énoncés contenus dans la demande de soumissions. Afin de faciliter l'évaluation de la soumission, le Canada demande que les soumissionnaires reprennent les sujets dans l'ordre des critères d'évaluation, sous les mêmes rubriques. Pour éviter les recoupements, les soumissionnaires peuvent faire référence à différentes sections de leur soumission en indiquant le numéro de l'alinéa et de la page où le sujet visé est déjà traité.

3.3 Section II : Soumission financière

A. Les soumissionnaires doivent présenter leur soumission financière en conformité avec le barème de prix décrit à la pièce jointe 1 de la partie 3. Le montant total des taxes applicables doit être indiqué séparément.

3.3.1 Paiement électronique de factures - soumission

A. Si vous êtes disposés à accepter le paiement de factures au moyen d'instruments de paiement électronique, compléter la pièce jointe 2 de la partie 3, Instruments de paiement électronique, afin d'identifier lesquels sont acceptés.

B. Si la pièce jointe 2 de la partie 3, Instruments de paiement électronique n'a pas été complétée, il sera alors convenu que le paiement de factures au moyen d'instruments de paiement électronique ne sera pas accepté.

C. L'acceptation des instruments de paiement électronique ne sera pas considérée comme un critère d'évaluation.

3.3.2 Fluctuation du taux de change

A. Le besoin ne prévoit pas offrir d'atténuer les risques liés à la fluctuation du taux de change. Aucune demande d'atténuation des risques liés à la fluctuation du taux de change ne sera prise en considération. Toute soumission incluant une telle disposition sera déclarée non recevable.

3.4 Section III : Attestations

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

3.5 Section IV : Renseignements supplémentaires

A. Dans la section IV de leur soumission, les soumissionnaires devraient fournir :

(i) page 1 de cette demande de soumissions, complétée, signée et datée;

(ii) le nom de la personne-ressource (fournir aussi son titre, son adresse postale, ses numéros de téléphone et de télécopieur, et son adresse courriel) autorisée par le soumissionnaire à communiquer avec le Canada en ce qui concerne leur soumission et tout contrat subséquent pouvant découler de leur soumission;

(iii) pour la partie 2, l'article 2.5, lois applicables de la demande de soumissions: la province ou le territoire si différent de celui spécifié;

(iv) concernant à l'article 6.1, Exigences relatives à la sécurité, de la Partie 6 de la demande de soumissions, pour chaque individu devant avoir accès à des renseignements ou à des biens de nature protégée ou classifiée, ou devant avoir accès à des établissements de travail dont l'accès est réglementé :

(a) le nom de chaque individu;

(b) la date de naissance de chaque individu; et

(b) si disponible, les renseignements confirmant que le individu satisfait aux exigences de sécurité, tel qu'indiqué à la Partie 7 - Clauses du contrat subséquent; et

(v) tout autre renseignement présenté dans la soumission qui n'a pas déjà été indiqué.

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

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

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

B. L'agent de sécurité d'entreprise (ASE) doit s'assurer, par l'entremise du Programme de sécurité industrielle (PSI) que le soumissionnaire et les individus proposés sont titulaires d'une cote de sécurité en vigueur et au niveau exigé, tel que décrit à la Partie 6 - Exigences relatives à la sécurité, exigences financières et autres exigences.

PIÈCE JOINTE 1 DE LA PARTIE 3 – BARÈME DE PRIX DÉCRIT

A. Le soumissionnaire doit remplir le barème de prix et le joindre à sa soumission financière.

B. Les données volumétriques figurant dans ce barème de prix sont communiquées uniquement aux fins de détermination du prix de la soumission évaluée. Elles ne doivent pas être considérées comme une garantie contractuelle. Leur inclusion dans ce barème de prix ne représente pas un engagement de la part du Canada que son utilisation future des services décrits dans la demande de soumissions correspondra à ces données.

C. Les prix unitaires fermes indiqués ci-dessous comprennent tous les frais qui pourraient être engagés pour répondre aux conditions de tout contrat découlant de la soumission, ce qui comprend le coût total des frais de déplacement et de subsistance qui peuvent être engagés pour réaliser les travaux décrits dans l'annexe A, Énoncé des besoins, de la demande de soumissions.

D. Le Canada n'acceptera aucuns frais de déplacement et de subsistance engagés dans tout contrat subséquent par l'entrepreneur relativement à toute réinstallation de ressources nécessaires au respect de ses obligations contractuelles.

E. Les prix et les coûts doivent être présentés en dollars canadiens, excluant les taxes applicables, DAP destination, incluant les frais de transport, excluant les droits de douane et les taxes d'accise canadiens.

1. Barème de prix décrit

Devise	$ CA

1.1 PÉRIODE INITIALE DU CONTRAT : DE LA DATE D'ATTRIBUTION DU CONTRAT AU 31 MARS 2024. TOUS LES ARTICLES DOIVENT ÊTRE LIVRÉS D'ICI LE 30 AOÛT 2023.

N^{O} DE L'ARTICLE	**DESCRIPTION**	**Q^{TÉ}**	**UNITÉ DE DISTRIBUTION**	**PRIX UNITAIRE FERME ($ CA)**	**PRIX ESTIMATIF TOTAL ($ CA)**
		(A)		**(B)**	**(C = A x B)**
1.0	**ÉQUIPEMENT**				
1.1	Sonde émettrice pour les congélateurs à -80 °C, avec certificat d'étalonnage, conformément au paragraphe 2.1.1.1 de l'annexe A	Jusqu'à 5	Unitaire	$	$
1.2	Sonde émettrice pour les congélateurs à -20 °C, avec certificat d'étalonnage, conformément au paragraphe 2.1.1.1 de l'annexe A	Jusqu'à 30	Unitaire	$	$

1.3	Sonde émettrice pour les réfrigérateurs entre 2 °C et 8 °C, avec certificat d'étalonnage, conformément au paragraphe 2.1.1.1 de l'annexe A	Jusqu'à 61	Unitaire	$	$
1.4	Passerelle de réception dotée d'un routeur du système mondial de communications mobiles (GSM), conformément au paragraphe 2.1.1.2 de l'annexe A	1	Lot	$	$
1.5	Progiciel pour l'ensemble des sondes émettrices, sans limites du nombre d'utilisateurs et du nombre d'alarmes (téléphone, courriel ou message texte), conformément au paragraphe 2.1.2.1 de l'annexe A	1	Unitaire	$	$
1.6	Forfait cellulaire pour l'ensemble des passerelles de réception, conformément au paragraphe 2.1.2.2 de l'annexe A	1	Unitaire	$	$
2.0	**FORMATION**				
2.1	Séance d'instruction virtuelle des opérateurs pour 5 à 10 opérateurs, conformément au paragraphe 9.1 de l'annexe A	Jusqu'à 30	Séance	$	$
2.2	Séance d'instruction sur le soutien technique pour 2 à 8 technologues en génie biomédical, conformément au paragraphe 9.2 de l'annexe A	1	Séance	$	$
			TOTAL DE LA PÉRIODE INITIALE DU CONTRAT		**$**

2.0 BESOINS OPTIONNELS DU 1ER AVRIL 2024 AU 31 MARS 2027 TOUS LES ARTICLES DOIVENT ÊTRE LIVRÉS D'ICI LE 31 MARS 2027.

2.1 BESOINS OPTIONNELS – ANNÉE 1 : DU 1ER AVRIL 2024 AU 31 MARS 2025

N° DE L'ARTICLE	DESCRIPTION	QTÉ	UNITÉ DE DISTRIBUTION	PRIX UNITAIRE FERME ($ CA)	PRIX ESTIMATIF TOTAL ($ CA)
		(A)		(B)	(C = A x B)
1.0	**ÉQUIPEMENT**				
1.1	Tout type de sondes émettrices pour les congélateurs à -80 °C ou à -20 °C, ou les réfrigérateurs entre 2 °C à 8 °C, avec certificat d'étalonnage, conformément au paragraphe 2.2.1.1 de l'annexe A	Jusqu'à 24	Unitaire	$	$
1.2	Passerelle de réception dotée d'un routeur GSM, conformément au paragraphe 2.2.1.2 de l'annexe A	Jusqu'à 6	Unitaire	$	$
1.3	Progiciel pour une (1) sonde émettrice supplémentaire, pour une période d'un (1) an, conformément au paragraphe 2.2.3.1 de l'annexe A	Jusqu'à 24	Unitaire	$	$
1.4	Forfait cellulaire pour une (1) passerelle de réception supplémentaire, pour une période d'un (1) an, conformément au paragraphe 2.2.3.3 de l'annexe A	Jusqu'à 6	Unitaire	$	$
1.5	Progiciel pour les sondes émettrices initiales, conformément au paragraphe 2.2.3.2 de l'annexe A	1	Unitaire	$	$
1.6	Forfait cellulaire pour les passerelles de réception initiales, conformément au paragraphe 2.2.3.4 de	1	Unitaire	$	$

	l'annexe A				
1.7	Étalonnage hors site des sondes, conformément au paragraphe 2.2.2.3 de l'annexe A	1	Service	$	$
2.0	**FORMATION**				
2.1	Séance d'instruction virtuelle des opérateurs pour 5 à 10 opérateurs, conformément au paragraphe 9.1 de l'annexe A	Jusqu'à 10	Séance	$	$
2.2	Séance d'instruction sur le soutien technique pour 2 à 8 technologues en génie biomédical, conformément au paragraphe 9.2 de l'annexe A	1	Séance	$	$
				TOTAL DES BESOINS OPTIONNELS – ANNÉE 1	**$**

2.2 BESOINS OPTIONNELS – ANNÉE 2 : DU 1ER AVRIL 2025 AU 31 MARS 2026

NO DE L'ARTICLE	**DESCRIPTION**	**QTÉ**	**UNITÉ DE DISTRIBUTION**	**PRIX UNITAIRE ($ CA)**	**TARIF CALCULÉ ($ CA)**
		(A)		**(B)**	**(C = A x B)**
1.0	**ÉQUIPEMENT**				
1.1	Tout type de sondes émettrices pour les congélateurs à -80 °C ou à -20 °C, ou les réfrigérateurs entre 2 °C à 8 °C, avec certificat d'étalonnage, conformément au paragraphe 2.2.1.1 de l'annexe A	Jusqu'à 24	Unitaire	$	$
1.2	Passerelle de réception dotée d'un routeur GSM, conformément au paragraphe 2.2.1.2 de l'annexe A	Jusqu'à 6	Unitaire	$	$

1.3	Progiciel pour une (1) sonde émettrice supplémentaire, pour une période d'un (1) an, conformément au paragraphe 2.2.3.1 de l'annexe A	Jusqu'à 48	Unitaire	$	$
1.4	Forfait cellulaire pour une (1) passerelle de réception supplémentaire, pour une période d'un (1) an, conformément au paragraphe 2.2.3.3 de l'annexe A	Jusqu'à 12	Unitaire	$	$
1.5	Progiciel pour les sondes émettrices initiales, conformément au paragraphe 2.2.3.2 de l'annexe A	1	Unitaire	$	$
1.6	Forfait cellulaire pour les passerelles de réception initiales, conformément au paragraphe 2.2.3.4 de l'annexe A	1	Unitaire	$	$
1.7	Étalonnage hors site des sondes, conformément au paragraphe 2.2.2.3 de l'annexe A	1	Service	$	$
2.0	**FORMATION**				
2.1	Séance d'instruction virtuelle des opérateurs pour 5 à 10 opérateurs, conformément au paragraphe 9.1 de l'annexe A	Jusqu'à 10	Séance	$	$
2.2	Séance d'instruction sur le soutien technique pour 2 à 8 technologues en génie biomédical, conformément au paragraphe 9.2 de l'annexe A	1	Séance	$	$
				TOTAL DES BESOINS OPTIONNELS – ANNÉE 2	**$**

2.3 BESOINS OPTIONNELS – ANNÉE 3 : DU 1ER AVRIL 2026 AU 31 MARS 2027

NO DE L'ARTICLE	DESCRIPTION	QTÉ	UNITÉ DE DISTRIBUTION	PRIX UNITAIRE ($ CA)	TARIF CALCULÉ ($ CA)
		(A)		(B)	(C = A x B)
1.0	**ÉQUIPEMENT**				
1.1	Tout type de sondes émettrices pour les congélateurs à -80 °C ou à -20 °C, ou les réfrigérateurs entre 2 °C à 8 °C, avec certificat d'étalonnage, conformément au paragraphe 2.2.1.1 de l'annexe A	Jusqu'à 24	Unitaire	$	$
1.2	Passerelle de réception dotée d'un routeur GSM, conformément au paragraphe 2.2.1.2 de l'annexe A	Jusqu'à 6	Unitaire	$	$
1.3	Progiciel pour une (1) sonde émettrice supplémentaire, pour une période d'un (1) an, conformément au paragraphe 2.2.3.1 de l'annexe A	Jusqu'à 72	Unitaire	$	$
1.4	Forfait cellulaire pour une (1) passerelle de réception supplémentaire, pour une période d'un (1) an, conformément au paragraphe 2.2.3.3 de l'annexe A	Jusqu'à 18	Unitaire	$	$
1.5	Progiciel pour les sondes émettrices initiales, conformément au paragraphe 2.2.3.2 de l'annexe A	1	Unitaire	$	$
1.6	Forfait cellulaire pour les passerelles de réception initiales, conformément au paragraphe 2.2.3.4 de l'annexe A	1	Unitaire	$	$

1.7	Étalonnage hors site des sondes, conformément au paragraphe 2.2.2.3 de l'annexe A	1	Service	$	$
2.0	**FORMATION**				
2.1	Séance d'instruction virtuelle des opérateurs pour 5 à 10 opérateurs, conformément au paragraphe 9.1 de l'annexe A	Jusqu'à 10	Séance	$	$
2.2	Séance d'instruction sur le soutien technique pour 2 à 8 technologues en génie biomédical, conformément au paragraphe 9.2 de l'annexe A	1	Séance	$	$
				TOTAL DES BESOINS OPTIONNELS – ANNÉE 3	**$**

3.0 PRIX TOTAL ÉVALUÉ (AUX FINS D'ÉVALUATION DE LA SOUMISSION)

DESCRIPTION	PRIX TOTAL ($ CA)
Total de la période initiale du contrat	_____ $
Total des besoins optionnels (année 1)	_____ $
Total des besoins optionnels (année 2)	_____ $
Total des besoins optionnels (année 3)	_____ $
PRIX ÉVALUÉ TOTAL	_____ **$**

PIÈCE JOINTE 2 DE LA PARTIE 3 – INSTRUMENTS DE PAIEMENT ÉLECTRONIQUE

A. Le soumissionnaire accepte d'être payé au moyen de l'un des instruments de paiement électronique suivants :

( ) Carte d'achat VISA;

( ) Carte d'achat MasterCard;

( ) Dépôt direct (national et international); et (ou)

( ) Virement télégraphique (international seulement).

PARTIE 4 – PROCÉDURES D'ÉVALUATION ET MÉTHODE DE SÉLECTION

4.1 Procédures d'évaluation

A. Les soumissions seront évaluées par rapport à l'ensemble des exigences de la demande de soumissions.

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

4.1.1 Évaluation technique

4.1.1.1 Critères techniques obligatoires

A. Les critères techniques obligatoires sont inclus dans la pièce jointe 1 de la partie 4.

4.1.2 Évaluation financière

A. Le prix de la soumission sera évalué comme suit :

(i) les soumissionnaires établis au Canada doivent proposer des prix fermes, les droits de douane et les taxes d'accise canadiens compris, et les taxes applicables exclues; et

(ii) les soumissionnaires établis à l'étranger doivent proposer des prix fermes, les droits de douane, les taxes d'accise canadiens et les taxes applicables exclus. Les droits de douane et les taxes d'accise canadiens payables par le Canada seront ajoutés, pour les besoins de l'évaluation seulement, aux prix présentés par les soumissionnaires établis à l'étranger.

B. Sauf lorsque la demande de soumissions précise que les soumissions doivent être présentées en dollars canadiens, les soumissions présentées en devises étrangères seront converties en dollars canadiens pour les besoins de l'évaluation. Pour les soumissions présentées en devises étrangères, le taux indiqué par la Banque du Canada à la date de clôture des soumissions, ou à une autre date précisée dans la demande de soumissions, sera utilisé comme facteur de conversion.

C. Bien que le Canada se réserve le droit d'attribuer le contrat FAB usine ou FAB destination, le Canada demande que les soumissionnaires proposent des prix FAB usine ou point d'expédition et FAB destination. Les soumissions seront évaluées sur une base FAB destination.

D. Pour les fins de la demande de soumissions, les soumissionnaires qui ont une adresse au Canada sont considérés comme étant des soumissionnaires établis au Canada, et les soumissionnaires qui ont une adresse à l'extérieur du Canada sont considérés comme étant des soumissionnaires établis à l'étranger.

4.2 Méthode de sélection - le prix évalué le plus bas, critères techniques obligatoires

A. Une soumission doit respecter les exigences de la demande de soumissions et satisfaire à tous les critères d'évaluation techniques obligatoires pour être déclarée recevable. La soumission recevable avec le prix évalué le plus bas sera recommandée pour attribution d'un contrat.

B. Si deux (2) soumissions recevables ou plus ont le même prix évalué le plus bas, la soumission qui est reçue en premier, en fonction de la date et de l'heure sera recommandée pour l’attribution d’un contrat.

PIÈCE JOINTE 1 DE LA PARTIE 4 – LES CRITÈRES D'ÉVALUATION TECHNIQUES

A. Une soumission doit respecter les exigences de la demande de soumissions et satisfaire à tous les critères d'évaluation techniques obligatoires pour être déclarée recevable. La soumission recevable avec le prix évalué le plus bas sera recommandée pour l'attribution d'un contrat.

B. Le soumissionnaire doit démontrer qu'il respecte les critères techniques obligatoires suivants à l'aide de documents à l'appui, comme une capture d'écran de la fonction de l'équipement, un manuel d'utilisateur, des brochures techniques ou de ventes, un rapport ou des attestations qui doivent être fournies dans sa soumission. Si le soumissionnaire ne fournit pas de documents à l'appui qui démontrent clairement qu'il respecte tous les critères techniques obligatoires, sa soumission peut être jugée non conforme et rejetée d'emblée. Les renseignements proposés à titre d'options ou d'ajouts à l'énoncé des travaux NE seront PAS évalués.

1. Critères techniques obligatoires

Nº	CRITÈRES TECHNIQUES OBLIGATOIRES	JUSTIFICATION DU SOUMISSIONNAIRE (INCLUANT LE LIEU DANS LA PROPOSITION; LE TITRE, LE Nº DE PAGE, ETC.)
CO1	Le soumissionnaire doit démontrer que le système de surveillance de l'environnement proposé est certifié par l'Association canadienne de normalisation (CSA) (https://www.csagroup.org/fr/services-dessai-et-de-certification/marques-et-etiquettes/) ou qu'il possède une preuve d'équivalence reconnue par le Conseil canadien des normes (CCN) (https://www.scc.ca/fr). Une preuve de certification ou une preuve d'équivalence doit être jointe à la soumission.	
CO2	Le soumissionnaire doit démontrer que le système de surveillance de l'environnement est prêt à transmettre des données à la plateforme Web à partir d'un réseau cellulaire et d'un réseau Ethernet. Pour prouver le respect du critère CO2, la soumission doit inclure une référence à la fiche de données, à la brochure ou au manuel.	
CO3	Le soumissionnaire doit démontrer que le système de surveillance de l'environnement proposé est capable de surveiller les éléments suivants : • la température des congélateurs; • la température des réfrigérateurs; • la température ambiante; • l'humidité; • les pannes de courant; • les inondations.	

	La soumission doit inclure une liste des capteurs compatibles avec les appareils de surveillance de l'environnement.	
CO4	Le soumissionnaire doit démontrer que le logiciel de surveillance de l'environnement proposé est capable de créer les profils d'utilisateur suivants : • administrateur; • superviseur; • utilisateur; • assurance de la qualité. La soumission doit inclure des captures d'écran montrant la marche à suivre pour créer différents profils d'utilisateur.	
CO5	Le soumissionnaire doit démontrer que le logiciel de surveillance de l'environnement est capable d'imposer des restrictions d'accès, de modification, d'ajout et de suppression à chaque profil d'utilisateur pour les paramètres suivants : • l'accès aux appareils; • les droits des utilisateurs. La soumission doit inclure des captures d'écran montrant la marche à suivre pour configurer les restrictions d'accès aux appareils dans les profils d'utilisateur.	
CO6	Pour les systèmes qui utilisent des sondes émettrices sans fil, le soumissionnaire doit démontrer que les systèmes respectent les exigences énoncées dans les cahiers des charges sur les normes radioélectriques d'Innovation, Sciences et Développement économique Canada (ISDE). Une preuve de certificat d'approbation technique doit être jointe à la soumission.	

PARTIE 5 – ATTESTATIONS ET RENSEIGNEMENTS SUPPLÉMENTAIRES

A. Les soumissionnaires doivent fournir les attestations et les renseignements supplémentaires exigés pour qu'un contrat leur soit attribué.

B. Les attestations que les soumissionnaires remettent au Canada peuvent faire l'objet d'une vérification à tout moment par le Canada. À moins d'indication contraire, le Canada déclarera une soumission non recevable, ou à un manquement de la part de l'entrepreneur s'il est établi qu'une attestation du soumissionnaire est fausse, sciemment ou non, que ce soit pendant la période d'évaluation des soumissions, ou pendant la durée du contrat.

C. L'autorité contractante aura le droit de demander des renseignements supplémentaires pour vérifier les attestations du soumissionnaire. À défaut de répondre et de coopérer à toute demande ou exigence imposée par l'autorité contractante, la soumission sera déclarée non recevable, ou constituera un manquement aux termes du contrat.

5.1 Attestations exigées avec la soumission

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

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

A. Conformément à la *Politique d'inadmissibilité et de suspension* (http://www.tpsgc-pwgsc.gc.ca/ci-if/politique-policy-fra.html), le soumissionnaire doit présenter avec sa soumission la documentation exigée, s'il y a lieu, afin que sa soumission ne soit pas rejetée du processus d'approvisionnement.

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

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

5.2.1 Dispositions relatives à l'intégrité - documentation exigée

A. Conformément à la *Politique d'inadmissibilité et de suspension* (http://www.tpsgc-pwgsc.gc.ca/ci-if/politique-policy-fra.html), le soumissionnaire doit présenter la documentation exigée, s'il y a lieu, afin que sa soumission ne soit pas rejetée du processus d'approvisionnement.

5.2.2 Exigences de sécurité – Documentation requise

Conformément aux exigences du Programme de sécurité des contrats de Travaux publics et Services gouvernementaux Canada (http://www.tpsgc-pwgsc.gc.ca/esc-src/introduction-fra.html), Les soumissionnaires basés au Canada doivent fournir le formulaire de demande d'inscription (FDI) du Programme de sécurité des contrats (PSC) dûment rempli, inclus dans la Pièce jointe 1 de la Partie 5, pour que leur candidature soit prise en considération dans le cadre du processus d'approvisionnement. Les soumissionnaires basés à l'étranger doivent remplir le formulaire de filtrage initial (FFI) de sécurité internationale du Programme de sécurité des contrats (PSC) dûment rempli, inclus dans la Pièce jointe 2

de la Partie 5, pour que leur candidature soit prise en considération dans le processus d'approvisionnement.

On rappelle aux soumissionnaires d'obtenir rapidement la cote de sécurité requise et, le cas échéant, les capacités en matière de sécurité. Comme il est indiqué ci-dessus, les soumissionnaires qui ne fournissent pas toutes les informations requises avec leurs soumissions auront la possibilité de compléter les informations manquantes du FDI OU FFI dans un délai fixé par l'autorité contractante. Si ces renseignements ne sont pas fournis dans le délai établi par l'autorité contractante (y compris toute prolongation accordée par l'autorité contractante à sa discrétion), ou si le Canada a besoin d'autres renseignements de la part de le soumissionnaire dans le cadre de l'évaluation de la demande d'autorisation de sécurité (c.-à-d. des renseignements qui ne sont pas exigés par le FDI OU FFI), le soumissionnaire sera tenu de soumettre ces renseignements dans le délai établi par l'autorité contractante, qui ne sera pas inférieur à 48 heures. Si, à quelque moment que ce soit, le soumissionnaire ne fournit pas les renseignements requis dans les délais fixés par l'autorité contractante, sa soumission sera déclarée non conforme.

5.2.3 Programme de contrats fédéraux pour l'équité en matière d'emploi - Attestation de soumission

A. En présentant une soumission, le soumissionnaire atteste que le soumissionnaire, et tout membre de la coentreprise si le soumissionnaire est une coentreprise, n'est pas nommé dans la liste des « soumissionnaires à admissibilité limitée du PCF » du Programme de contrats fédéraux (PCF) pour l'équité en matière d'emploi disponible au bas de la page du site Web d'Emploi et Développement social Canada (EDSC) - Travail (https://www.canada.ca/fr/emploi-developpement-social/programmes/equite-emploi/programme-contrats-federaux.html).

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

National Defence | Défense nationale

National Defence Headquarters
Ottawa, Ontario
K1A 0K2

Quartier général de la Défense nationale
Ottawa (Ontario)
K1A 0K2

PIÈCE JOINTE 1 DE LA PARTIE 5 – PROGRAMME DE SÉCURITÉ DES CONTRATS (PSC)
FORMULAIRE DE DEMANDE D'INSCRIPTION (FDI)

Les soumissionnaires représentant des organisations basées au Canada doivent remplir le FDI suivant dans le cadre de leur soumission. Si le FDI ne fait pas partie de la soumission, l'autorité contractante peut en demander une copie avant l'attribution du contrat :

Programme de sécurité des contrats (PSC) - Demande d'inscription (DI) (pwgsc.gc.ca)

PIÈCE JOINTE 2 DE LA PARTIE 5 – PROGRAMME DE SÉCURITÉ DES CONTRATS (PSC) FORMULAIRE DE FILTRAGE INITIAL (FFI) DE SÉCURITÉ INTERNATIONALE

Les soumissionnaires représentant des organisations basées à l'étranger doivent remplir le FFI suivant dans le cadre de leur soumission. Si le FFI ne fait pas partie de la soumission, l'autorité contractante peut en demander une copie avant l'attribution du contrat :

Object

Le présent formulaire a pour objet d'amorcer le processus de contrôle de sécurité pour les fournisseurs étrangers qui auront besoin d'avoir accès à des renseignements, des biens ou des sites protégés/classifiés canadiens dans le cadre d'un contrat ou d'un programme multinational du gouvernement du Canada traité par le Programme de sécurité des contrats (CSP) canadien. Les renseignements fournis pourraient être divulgués à la Gendarmerie royale du Canada et au Service canadien du renseignement de sécurité dans le but de mener les vérifications et/ou les enquêtes requises. Les renseignements pourraient aussi être communiqués à d'autres institutions fédérales qui pourraient avoir besoin de les utiliser pour s'acquitter de leurs fonctions ou pour mener des enquêtes conformément aux lois canadiennes, ou aux programmes de sécurité industrielle de gouvernements étrangers.

Le rôle de l'Autorité désignée de la sécurité pour le Canada (ADS canadien) est exécuté par la Direction de la sécurité industrielle internationale dans le cadre du Programme de sécurité des contrats et est l'autorité canadienne chargée de confirmer la conformité aux exigences canadiennes en matière de sécurité nationale et internationale auxquelles participent des fournisseurs étrangers.

Consignes pour remplir le formulaire de filtrage initial

Généralités

- Ce formulaire et les documents supplémentaires requis doivent être fournis en français ou en anglais.
- Si vous n'avez pas assez de place pour fournir une réponse complète dans une des sections de ce formulaire, veuillez inclure des pages et/ou des lignes supplémentaires dans les tableaux au besoin.
- Le fait de fournir des renseignements faux ou trompeurs ou de dissimuler ou d'omettre de déclarer tout fait important dans le cadre de cette demande de filtrage initial vous rendra immédiatement inadmissible à exécuter les contrats et les programmes multinationaux nécessitant l'accès à des renseignements, des biens ou des sites protégés/classifiés canadiens.

Section A – Renseignements sur l'entreprise

- Vous devez fournir toute la documentation requise (décrite ci-dessous) relativement au type d'entreprise ou de la personne morale. L'organigramme de l'entreprise ou de la personne morale est obligatoire pour tous les types d'organisation.
- **Dénomination sociale de l'entreprise ou de la personne morale** fait référence à la dénomination sociale de l'entreprise ou de la personne morale telle qu'elle est enregistrée auprès des autorités gouvernementales étrangères compétentes.
- Le **nom de l'organisation ou nom commercial** fait référence au nom sous lequel une entreprise exerce une activité commerciale, bien que la dénomination sociale sous laquelle elle est inscrite, qui est utilisée pour les contrats et divers contextes officiels, puisse être différente.
- Une **société** désigne une entité qui est autorisée en vertu de la loi d'agir en tant que personne individuelle et distincte des actionnaires qui en sont propriétaires, et détenant le droit d'émettre des actions et d'exister indéfiniment. Fournissez les informations suivantes pour justifier cette sélection d'entreprise ou de personne morale :
    - Identificateur de bourse des valeurs (le cas échéant); et
    - Certificat de constitution, de conformité ou de prorogation.
- Un **partenariat** désigne un contrat volontaire entre au moins deux personnes compétentes visant à mettre en commun leur argent, leurs effets, leur travail et leurs habiletés, en partie ou en totalité, pour s'adonner au commerce ou à des activités licites et en partager entre elles les profits et les pertes de façon

proportionnelle. Fournissez les informations suivantes pour justifier cette sélection d'entreprise ou de personne morale :

- Documentation à l'appui du statut juridique.

- Une **entreprise à propriétaire unique** désigne le propriétaire d'une entreprise qui agit seul et qui n'a pas de partenaire. Fournissez les informations suivantes pour justifier cette sélection d'entreprise ou de personne morale :

  - Une preuve des détails de l'inscription gouvernementale; et
  - Autre permis (p.ex. le permis principal d'entreprise).

- Une **société d'État** désigne une entreprise d'État ou une entreprise publique dont le gouvernement ou l'État a un contrôle important sur cette entité commerciale par le biais d'une propriété entièrement, majoritaire ou importante d'une minorité. Fournissez les informations suivantes pour justifier cette sélection d'entreprise ou de personne morale :

  - Une loi nationale, acte législative ou une politique gouvernementale définissant la société d'État; et
  - Documentation à l'appui du statut juridique.

- **Autre** (p.ex. lettres patentes, universités, institutions financières, organisations non constituées en société) Fournissez les informations suivantes pour justifier cette sélection d'entreprise ou de personne morale :

  - Preuve du status juridique;
  - lois nationales ou actes législatives; et/ou
  - Chartes.

- Si l'entreprise ou la personne morale est déjà inscrite à un programme de sécurité industrielle de l'Autorité nationale de sécurité (ANS) ou de l'Autorité désignée de sécurité (ASD) du pays concerné, indiquer le niveau de l'attestation de sécurité des installations et sa date de validité s'il y a lieu.

- Indiquer le nom de l'Autorité de protection des données (APD) responsable de la protection des renseignements personnels dans le pays où se trouve l'entreprise ou personne morale et le titre de la loi régissant cette Autorité.

Section B – Agent de sécurité de l'entreprise (ASER)

- Nommez la personne que vous prévoyez désigner en tant qu'Agent de sécurité de l'entreprise (ASER) qui sera responsable d'assurer le respect des exigences de sécurité du contrat du gouvernement du Canada ou du programme multinational.

- L'ASER **doit** :

  - être un employé de l'entreprise ou personne morale; et
  - être évalué au même niveau de sécurité que l'entreprise ou la personne morale.

- L'ASER doit aviser le Programme de sécurité des contrats de tout changement de structure de la propriété de la société ou de la personne morale, y compris les changements de composition de son conseil d'administration et le changement de l'ASER désigné.

- La **citoyenneté** fait référence au statut de citoyen. Un citoyen est une personne qui, par naissance ou naturalisation, est membre d'une communauté politique, doit allégeance à la communauté et a le droit de jouir de tous les droits et protections civil.

- Aux fins du Programme de sécurité des contrats, le terme « **pays de résidence principale/domicile national** » désigne le pays où la personne a établi son domicile véritable, fixe, principal et permanent, et auquel cette personne a l'intention de retourner et de rester même si elle réside actuellement ailleurs.

Section C – Conseil d'administration

- Faire une liste de tous les membres du conseil d'administration de l'organisation. Ajouter des lignes supplémentaires à la section au besoin.

- La **citoyenneté** fait référence au statut de citoyen. Un citoyen est une personne qui, par naissance ou naturalisation, est membre d'une communauté politique, doit allégeance à la communauté et a le droit de jouir de tous les droits et protections civil.

- Aux fins du Programme de sécurité des contrats, le terme « **pays de résidence principale/domicile national** » désigne le pays où la personne a établi son domicile véritable, fixe, principal et permanent, et auquel cette personne a l'intention de retourner et de rester même si elle réside actuellement ailleurs.

Section D – Information sur les propriétaires

- Aux fins du Programme de sécurité des contrats, les définitions suivantes s'appliquent :

    - Les **propriétaires directs (ou inscrits)** sont des propriétaires qui détiennent le titre juridique d'une propriété ou d'un bien à leur nom.
    - La **propriété** se réfère soit (1) aux droits de vote liés aux actions avec droit de vote en circulation de l'entreprise ou personne morale ou (2) aux actions en circulation mesurées selon la juste valeur marchande.
    - Une **société mère** désigne une entreprise qui détient et/ou contrôle la participation majoritaire (c.-à-d. les actions avec droit de vote) d'autres firmes ou entreprises, habituellement connues sous le nom de filiales, ce qui peut lui donner le contrôle des opérations de celles-ci.

Section E – Attestation et consentement

- Seule une personne dont le nom figure à la Section C peut remplir cette section.

REMARQUE : Le fait de fournir des renseignements faux ou trompeurs ou de dissimuler ou d'omettre de déclarer tout fait important dans le cadre de cette demande de filtrage initial vous rendra immédiatement inadmissible à exécuter les contrats et les programmes multinationaux nécessitant l'accès à des renseignements, des biens ou des sites protégés/classifiés canadiens. Un formulaire incomplet ne sera pas traité et vous sera renvoyé.

SECTION A – RENSEIGNEMENTS SUR L'ENTREPRISE
Remplissez la section A et fournissez la documentation requise identifiée dans les instructions ci-dessus.
1. Dénomination sociale de l'entreprise ou personne morale
2. Nom de l'organisation ou nom commercial (si différent de la dénomination sociale)
3. Type d'entreprise ou de personne morale (Indiquez le type d'organisation et fournir les documents de validation requis) (sélectionner un seul) ☐ Entreprise à propriétaire unique ☐ Partenariat ☐ Société (privée ou publique) ☐ Société d'État ☐ Autre (veuillez préciser) :

4. Veuillez fournir une brève description des activités générales de l'entreprise		
5. Adresse municipale de l'entreprise (siège social)		
6. Adresse postale (si différente de l'adresse municipale de l'entreprise)		
7. Site Web de l'entreprise (le cas échéant)		
8. Numéro d'entreprise, le cas échéant (p.ex. code CAGE/NCAGE)	9. Numéro de téléphone (inclure le code du pays et le poste, le cas échéant)	10. Numéro de télécopieur, le cas échéant (inclure le code du pays)
11. Nombre d'employés dans l'entreprise		12. Nombre d'employés devant accéder à des renseignements, des biens ou des sites protégés/classifiés canadiens
13. Indiquez le niveau de sécurité de l'attestation valide de sécurité des installations de l'entreprise accordée par l'Autorité nationale de sécurité ou l'Autorité désignée de sécurité (inscrire NIL si aucune)		14. Le cas échéant, fournir la date d'échéance de l'attestation de sécurité des installations
15. Indiquez le nom de l'Autorité de protection des données (APD) responsable pour la protection de l'information personnelle dans le pays (inscrire NIL si aucune)		16. Le cas échéant, fournir le nom de la loi régissant l'Autorité de protection des données (APD)

SECTION B – AGENT DE SECURITÉ DE L'ENTREPRISE				
Remplissez la Section B.				
Titre du poste	Nom	Prénom(s)	Citoyenneté(s)	Pays de résidence principale/domicile
Adresse courriel de l'agent de sécurité de l'entreprise :				

SECTION C – LISTE DES MEMBRES DU CONSEIL D'ADMINISTRATION (INSCRIRE S.O. SI AUCUN CONSEIL)				
Remplissez la Section C. (Ajouter des lignes supplémentaires ou des pièces jointes au besoin)				
Titre du poste	Nom	Prénom(s)	Citoyenneté(s)	Pays de résidence principale/domicile

SECTION D – INFORMATION SUR LES PROPRIÉTAIRES

Remplissez la Section D correspondante pour chacun des niveaux de propriété
Indiquez toutes les entités, les personnes et les sociétés privées ou publiques qui détiennent des intérêts dans l'organisation indiquée à la Section 1. Pour les sociétés cotées en bourse, indiquez le marché boursier. Un tableau des relations entre les propriétaires avec des pourcentages de propriété doit aussi être fourni.

SECTION D-1 –NIVEAU 1 DE PROPRIÉTÉ (PROPRIÉTÉ DIRECTE)

Identifiez ci-dessous tous les propriétaires individuels ou la/les organisation(s) en lien directe(s) avec l'entreprise de la Section 1.

Nom de l'organisation ou de la personne	Adresse	Type d'entité (p.ex. société privée ou publique, de l'État)	Marché boursier public ou privé	Percentage de propriété	Territoire de juridiction (pays) ou citoyenneté(s)

SECTION D-2 – NIVEAU 2 DE PROPRIÉTÉ

S'il y a des propriétaires additionnels pour les noms mentionnés dans la section précédente (D-1), veuillez fournir les informations ci-dessous. Dans le cas contraire, veuillez inscrire la mention S.O. (sans objet).

Nom de l'organisation ou de la personne	Adresse	Type d'entité (p.ex. société privée ou publique, de l'État)	Marché boursier public ou privé	Percentage de propriété	Territoire de juridiction (pays) ou citoyenneté(s)

SECTION D-3 – NIVEAU 3 DE PROPRIÉTÉ

S'il y a des propriétaires additionnels pour les noms mentionnées dans la section précédente (D-2), veuillez fournir les informations ci-dessous. Dans le cas contraire, veuillez inscrire la mention S.O. (sans objet).

Nom de l'organisation ou de la personne	Adresse	Type d'entité (p. ex. société privée ou publique, de l'État)	Marché boursier public ou privé	Percentage de propriété	Territoire de juridiction (pays) ou citoyenneté(s)

SECTION E – ATTESTATION ET CONSENTEMENT
(seule une personne mentionnée à la section C peut remplir cette section)

Je soussigné(e), en tant que personne autorisée par l'organisation mentionnée à la Section 1, ai lu l'avis de confidentialité lié à cette demande et atteste par la présente que les renseignements qui y sont contenus sont vrais, complets et exacts. Je reconnais les responsabilités énoncées dans le Manuel de la sécurité industrielle de Services publics et Approvisionnement Canada et je conviens de m'y conformer, et je consens à la collecte, à l'utilisation et à la divulgation des renseignements fournis dans ce formulaire de filtrage initial aux fins décrites ci-dessus. Je conviens d'aviser le Programme de sécurité des contrats de tout changement à l'organisation, y compris un changement d'adresse, de numéros de téléphone, d'adresses courriels, de la structure organisationnelle, relatif à la propriété, d'agent de sécurité.de l'entreprise et des membres du Conseil d'administration.

National Defence | Défense nationale

National Defence Headquarters
Ottawa, Ontario
K1A 0K2

Quartier général de la Défense nationale
Ottawa (Ontario)
K1A 0K2

Nom	Prénom(s)
Titre du poste	Numéro de téléphone (inclure le code du pays et le numéro du poste s'il y a lieu)
Numéro de télécopieur s'il y a lieu (include le code du pays)	Adresse courriel
Signature	Date

UTILISATION RÉSERVÉE AU PROGRAMME DE SÉCURITÉ DES CONTRATS DE SPAC		
Recommandations		
Recommandation de l'analyste (nom)	Signature	Date
Approbation (nom)	Signature	Date

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

6.1 Exigences relatives à la sécurité

1. Avant l'attribution d'un contrat, les conditions suivantes doivent être respectées :

   (a) le soumissionnaire doit détenir une attestation de sécurité d'organisme valable tel qu'indiqué à la Partie 7 – Clauses du contrat subséquent;

   (b) le soumissionnaire doit fournir l'adresse des lieux proposés pour la réalisation des travaux et la sauvegarde des documents, tel qu'indiqué à la Partie 3 – section IV Renseignements supplémentaires.

2. Avant de donner accès à des renseignements de nature délicate au soumissionnaire, les conditions suivantes doivent être respectées:

   (a) les personnes proposées par le soumissionnaire devant avoir accès à des renseignements ou à des biens de nature délicate ou à des lieux de travail dont l'accès est réglementé doivent répondre aux exigences de sécurité indiquées à la partie 7 – Clauses du contrat subséquent;

   (b) les capacités en matière de sécurité du soumissionnaire doivent être satisfaites comme il est indiqué à la partie 7, Clauses du contrat subséquent;

3. Pour de plus amples renseignements sur les exigences relatives à la sécurité, les soumissionnaires devraient consulter le site Web du Programme de sécurité des contrats de Travaux publics et Services gouvernementaux Canada (http://www.tpsgc-pwgsc.gc.ca/esc-src/introduction-fra.html).

PARTIE 7 – CLAUSES DU CONTRAT SUBSÉQUENT

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

ARTICLES DE LA CONVENTION

7.1 Énoncé des Besoins

A. L'entrepreneur doit exécuter les travaux conformément à l'énoncé des travaux qui se trouve à l'annexe « A ».

7.2 Clauses et conditions uniformisées

A. Toutes les clauses et conditions identifiées dans le contrat par un numéro, une date et un titre sont reproduites dans le *Guide des clauses et conditions uniformisées d'achat* (https://achatsetventes.gc.ca/politiques-et-lignes-directrices/guide-des-clauses-et-conditions-uniformisees-d-achat) publié par Travaux publics et Services gouvernementaux Canada.

7.2.1 Conditions générales

A. 2030 (2022-05-12), Conditions générales - besoins plus complexes de biens, s'appliquent au contrat et en font partie intégrante, avec les modifications suivantes :

(i) L'article 01, Interprétation, « Canada », « Couronne », « Sa Majesté » ou « État », est supprimé en entier et remplacé par ce qui suit :

« Canada », « Couronne », « Sa Majesté » ou « État »
signifient Sa Majesté du chef du Canada représentée par le ministre de la Défense nationale et toute autre personne qui agit au nom du ministre ou, le cas échéant, un ministre compétent auquel le ministre de la Défense nationale a délégué ses pouvoirs ou ses fonctions, et toute autre personne dûment autorisée à agir au nom de ce ministre.

B. 2035 (2022-05-12), Conditions générales - besoins plus complexes de services, s'appliquent au contrat et en font partie intégrante, avec les modifications suivantes :

(i) L'article 01, Interprétation, « Canada », « Couronne », « Sa Majesté » ou « État », est supprimé en entier et remplacé par ce qui suit :

« Canada », « Couronne », « Sa Majesté » ou « État »
signifient Sa Majesté du chef du Canada représentée par le ministre de la Défense nationale et toute autre personne qui agit au nom du ministre ou, le cas échéant, un ministre compétent auquel le ministre de la Défense nationale a délégué ses pouvoirs ou ses fonctions, et toute autre personne dûment autorisée à agir au nom de ce ministre.

7.2.2 Conditions générales supplémentaires

A. Les conditions générales supplémentaires suivant s'appliquent au contrat et en font partie intégrante :

(i) 4001 (2015-04-01), Achat, location et maintenance de matériel;

(ii) 4003 (2010-08-16), Logiciels sous licence;

(iii) 4004 (2013-04-25), Services de maintenance et de soutien des logiciels sous licence;

(iv) 4006 (2010-08-16), L'entrepreneur détient les droits de propriété intellectuelle sur les renseignements originaux;

7.3 Exigences relatives à la sécurité

A. Les exigences relatives à la sécurité suivantes (LVERS et clauses connexes, tel que prévu par le PSI) s'appliquent et font partie intégrante du contrat :

(i) L'entrepreneur ou l'offrant doit détenir en permanence, pendant l'exécution du contrat ou de l'offre à commandes, une attestation de vérification d'organisation désignée (VOD) en vigueur, ainsi qu'une cote de protection des documents approuvée au niveau PROTÉGÉ A, délivrées par le Programme de sécurité des contrats (PSC), Travaux publics et Services gouvernementaux Canada (TPSGC).

(ii) Les membres du personnel de l'entrepreneur ou de l'offrant devant avoir accès à des renseignements ou à des biens PROTÉGÉS, ou à des établissements dont l'accès est réglementé, doivent TOUS détenir une cote de sécurité du personnel valable au niveau SECRET, ou FIABILITE, comme requis par le guide de sécurité, approuvée par la PSC de TPSGC.

(iii) L'entrepreneur NE DOIT PAS utiliser ses propres systèmes informatiques pour traiter, produire ou stocker électroniquement des renseignements ou des données et(ou) de production au niveau PROTÉGÉ jusqu'à ce que l'autorisation écrite a été émise par l'autorité en matière de sécurité pour le ministère ou agence du client. Lorsque cette autorisation aura été délivrée, ces tâches pourront être exécutées au niveau PROTÉGÉ A.

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

(v) L'entrepreneur ou l'offrant doit se conformer aux dispositions des documents suivants :

a) de la Liste de vérification des exigences relatives à la sécurité et directive de sécurité (s'il y a lieu), reproduite ci-joint à l'Annexe C;
b) le Manuel de la sécurité des contrats (dernière édition);
c) Site Web du PSC : Exigences de sécurité des contrats du gouvernement du Canada, veuillez visitez https://www.tpsgc-pwgsc.gc.ca/esc-src/index-fra.html

7.3.1 Installations ou locaux de l'entrepreneur nécessitant des mesures de sauvegarde

A. Lorsque des mesures de sauvegarde sont nécessaires pour réaliser les travaux, l'entrepreneur doit diligemment tenir à jour les renseignements relatifs à ses installations ou à ses locaux, et ceux des individus proposés pour les adresses suivantes :

[À préciser dans le contrat subséquent]

B. L'agent de sécurité d'entreprise (ASE) doit s'assurer, par l'entremise du Programme de sécurité industrielle (PSI) (http://ssi-iss.tpsgc-pwgsc.gc.ca/index-fra.html) que le soumissionnaire et les individus proposés sont titulaires d'une cote de sécurité en vigueur et au niveau exigé.

7.4 Durée du contrat

7.4.1 Période du contrat

A. La période du contrat est à partir de la date du contrat jusqu'au 31 mars 2027 inclusivement.

7.4.2 Date de livraison

A. Tous les biens livrables pour la période initiale du contrat doivent être reçus au plus tard le 30 août 2023. Tous les livrables pour le besoin facultatif, nécessaires « au fur et à mesure des besoins », doivent être livrés avant le 31 mars 2027.

7.4.3 Points de livraison

A. La livraison du besoin sera effectuée aux points de livraison identifiés à l'Annexe « A », Énoncé des Besoins du contrat.

7.5 Responsables

7.5.1 Autorité contractante

A. L'autorité contractante pour le contrat est :

Nom : Lana Ibrahim
Titre : Agente d'approvisionnement Sénior, D C Svcs 3-4-2
Direction : Direction des contrats de service 3 (D C Svcs 3)
Adresse : Le ministre de la Défense nationale (MDN)
101 Colonel By Drive
Ottawa ON K1A 0K2
Téléphone : _____
Courriel : Lana.Ibrahim@forces.gc.ca

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

7.5.2 Responsable technique

A. Le responsable technique pour le contrat est :

[À préciser dans le contrat subséquent]
Nom : _____
Titre : _____
Direction : _____
Adresse : Le ministre de la Défense nationale (MDN)
101 Colonel By Drive
Ottawa ON K1A 0K2
Téléphone : _____
Courriel : _____

B. Le responsable technique représente le ministère ou organisme pour lequel les travaux sont exécutés dans le cadre du contrat. Il est responsable de toutes les questions liées au contenu

technique des travaux prévus dans le contrat. On peut discuter des questions techniques avec le responsable technique; cependant, celui-ci ne peut pas autoriser les changements à apporter à l'énoncé des travaux. Ces changements peuvent être effectués uniquement au moyen d'une modification au contrat émise par l'autorité contractante.

7.5.3 Représentant de l'entrepreneur

[À préciser dans le contrat subséquent]
Nom : _____
Titre : _____
Adresse : _____
_____
_____
Téléphone : _____
Courriel : _____

7.6 Paiement

7.6.1 Base de paiement- Prix ferme

A. À condition de remplir de façon satisfaisante toutes ses obligations en vertu du contrat, l'entrepreneur sera payé un prix ferme précisé dans l'annexe «B », selon un montant total de _____ $ (insérer le montant au moment de l'attribution du contrat). Les droits de douane sont exclus et les taxes applicables sont en sus.

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

7.6.2 Limite de prix

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

7.6.3 Méthode de paiement-Paiements multiples

A. Le Canada paiera l'entrepreneur lorsque des unités auront été complétés et livrés conformément aux dispositions de paiement du contrat si :

i. une facture exacte et complète ainsi que tout autre document exigé par le contrat ont été soumis conformément aux instructions de facturation prévues au contrat;

ii. tous ces documents ont été vérifiés par le Canada;

iii. les travaux livrés ont été acceptés par le Canada.

7.6.4 Taxes - entrepreneur établi à l'étranger

A. Sauf indication contraire dans le contrat, le prix ne comprend aucune taxe fédérale d'accise, taxe locale ou d'état, de vente ou d'utilisation, aucune autre taxe de nature semblable, ni autre taxe canadienne, quelle qu'elle soit. Le prix comprend toutefois toutes les autres taxes. Si les travaux

sont normalement assujettis à la taxe fédérale d'accise, le Canada fournira à l'entrepreneur, sur demande, un certificat d'exemption de ladite taxe fédérale d'accise sous la forme prescrite par les règlements fédéraux.

Le Canada fournira à l'entrepreneur les preuves d'exportation qui peuvent être demandées par les autorités fiscales. Si le Canada omettait de le faire, et qu'en conséquence l'entrepreneur doit payer la taxe fédérale d'accise, le Canada remboursera l'entrepreneur si l'entrepreneur prend les mesures que le Canada peut exiger pour recouvrer tout paiement effectué par l'entrepreneur. L'entrepreneur doit rembourser au Canada tout montant ainsi recouvré**.**

7.6.5 Clauses du Guide des CCUA

A. C2608C, (2020-08-01), Documentation des douanes canadiennes
B. C2610C, (2007-11-30), Droits de douane- Ministère de la Défense nationale est l'importateur

7.6.6 Paiement électronique de factures - contrat

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

[À préciser dans le contrat subséquent]

(i) Carte d'achat Visa;

(ii) Carte d'achat MasterCard;

(iii) Dépôt direct (national et international);et

(iv) Virement télégraphique (international seulement).

7.7 Instructions relatives à la facturation

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

B. Chaque facture doit être appuyée par :

(i) une copie des feuilles de temps pour corroborer le temps de travail réclamé;

(ii) une copie du document de sortie et de tout autre document tel qu'il est spécifié au contrat;

(iii) une copie des factures, reçus, pièces justificatives pour tous les frais directs et pour tous les frais de déplacement et de subsistance;

C. Les factures doivent être distribuées comme suit :

(i) L'originale et un (1) exemplaire doivent être envoyés à l'adresse qui apparaît à la page 1 du contrat pour attestation et paiement.

(ii) Un (1) exemplaire doit être envoyé à l'autorité contractante identifiée sous l'article intitulé « Responsables » du contrat.

7.8 Attestations et renseignements supplémentaires

7.8.1 Conformité

A. À moins d'indication contraire, le respect continu des attestations fournies par l'entrepreneur avec sa soumission ou préalablement à l'attribution du contrat, ainsi que la coopération constante quant aux renseignements supplémentaires, sont des conditions du contrat et leur non-respect constituera un manquement de la part de l'entrepreneur. Les attestations pourront faire l'objet de vérifications par le Canada pendant toute la durée du contrat.

7.9 Lois applicables

A. Le contrat doit être interprété et régi selon les lois en vigueur en Ontario [ou à préciser dans le contrat subséquent] et les relations entre les parties seront déterminées par ces lois.

7.10 Ordre de priorité des documents

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

(i) Les articles de la convention;

(ii) Les conditions générales supplémentaires;
   a) 4001 (2015-04-01), Achat, location et maintenance de matériel;
   b) 4003 (2010-08-16), Logiciels sous licence;
   c) 4004 (2013-04-25), Services de maintenance et de soutien des logiciels sous licence;
   d) 4006 (2010-08-16), L'entrepreneur détient les droits de propriété intellectuelle sur les renseignements originaux

(iii) Les conditions générales 2030 (2022-05-12), Conditions générales - besoins plus complexes de biens;

(iv) Les conditions générales 2035 (2022-05-12), Conditions générales - besoins plus complexes de services;

(v) L'Annexe « A », Énoncé des besoins;

(vi) L'Annexe « B », Base de paiement;

(vii) L'Annexe « C », Liste de vérification des exigences relatives à la sécurité;

(viii) La soumission de l'entrepreneur datée du [à préciser dans le contrat subséquent], clarifiée le [à préciser dans le contrat subséquent], et modifiée le [à préciser dans le contrat subséquent].

7.11 Contrat de défense

A. Le contrat est un contrat de défense au sens de la *Loi sur la production de défense*, L.R.C. 1985, ch. D-1 (http://laws-lois.justice.gc.ca/fra/lois/d-1/), et est régi par cette loi.

B. Le droit de propriété sur les travaux ou les matériaux, pièces, travaux en cours ou achevés, appartient au Canada, libre et quitte de tout privilège, réclamation, charge, sûreté ou servitude.

Le Canada peut, à tout moment, retirer, vendre ou aliéner les travaux en tout ou en partie conformément à l'article 20 de la *Loi sur la production de défense*.

7.12 Marchandises excédentaires

A. La quantité de marchandise que l'entrepreneur doit livrer est spécifiée dans le contrat. L'entrepreneur demeure responsable des marchandises excédentaires livrées, peu importe si ces marchandises ont été livrées volontairement ou suite à une erreur de la part de l'entrepreneur. Le Canada ne paiera pas l'entrepreneur pour la livraison de marchandises excédentaires, et il ne retournera pas lesdites marchandises à l'entrepreneur, sauf si ce dernier accepte de payer tous les coûts liés à leur retour, y compris, sans toutefois s'y limiter, les coûts administratifs, d'expédition et de manutention. Le Canada se réserve le droit de déduire ces coûts de toute facture présentée par l'entrepreneur.

7.13 Règlements concernant les emplacements des Forces canadiennes

A. L'entrepreneur doit se conformer à tous les ordres ou autres règlements, instructions et directives en vigueur à l'emplacement où les travaux sont exécutés.

7.14 Livraison et déchargement

A. Les camions de livraison doivent être munis d'un dispositif permettant d'effectuer le déchargement dans les endroits dépourvus d'installation de déchargement hydraulique, fixe ou autre.

B. Au moment des livraisons, il doit y avoir un nombre d'employés suffisant pour décharger tous les types de véhicules sans l'aide des employés du gouvernement fédéral.

C. À certains endroits, les camions de livraison doivent être déchargés lorsqu'ils sont stationnés en bordure du trottoir. Lorsque le matériel est déposé sur le trottoir, il doit être placé à proximité de l'entrée désignée pour que le personnel de l'endroit puisse le transporter facilement à l'aide de l'équipement de manutention mécanique.

7.15 Marquage

A. L'entrepreneur doit s'assurer que le nom du fabricant et le numéro de pièce sont clairement estampillés ou gravés sur chaque article aux fins d'identification formelle.

7.16 Étiquetage

A. L'entrepreneur doit s'assurer que les numéros du fabricant et de la spécification apparaissent sur chaque article, soit imprimés sur le conteneur ou sur une étiquette adhésive rencontrant la plus haute norme commerciale apposée sur le conteneur.

7.17 Palettisation

A. Pour tous les envois qui excèdent 0,566 m3 ou 15,88 kg (20 pi3 ou 35 lbs), à l'exception des envois faits par messageries, les conditions suivantes s'appliquent :

i. L'entrepreneur doit cercler, et au besoin envelopper, les marchandises sur des palettes de bois standard de 1,22 m x 1,02 m (48 po x 40 po). La palette à quatre entrées doit être fournie, sans frais, au ministère de la Défense nationale. La hauteur totale, palettes y compris, ne doit pas dépasser 1,19 m (47 po). La charge unitaire ne doit pas dépasser aucun bords de la palette de plus de 2,54 cm (1 po).

ii. L'entrepreneur doit regrouper les articles identifiés d'un même numéro de stock (sur la même palette). Les palettes composées de plus d'un numéro de stock doivent être identifiées « Articles mixtes ».

iii. Les articles individuels mesurant plus de 1,22 m (48 po) de longueur ou pesant plus de 453,6 kg (1000 lbs) doivent être arrimés à des palettes plus larges ou doivent être montés sur des patins de 10,16 cm x 10,16 cm (4 po x 4 po) bien attachés au bas de l'article. Les patins doivent être séparés par un minimum de 71,12 cm (28 po).

B. Toute exception à ces exigences doit être approuvée au préalable par l'autorité contractante

Une (1) des deux (2) options suivantes sera insérée dans le contrat subséquent, selon le cas :

Option 1: A2000C (2006-06-16) lorsque le contrat sera conclu avec un fournisseur canadien; ou

7.18 Ressortissants étrangers (entrepreneur canadien)

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

Option 2: A2001C (2006-06-16) lorsque le contrat sera conclu avec un fournisseur établi à l'étranger.

7.18 Ressortissants étrangers (entrepreneur étranger)

A. L'entrepreneur doit se conformer aux exigences canadiennes en matière d'immigration relatives aux ressortissants étrangers qui doivent séjourner temporairement au Canada pour exécuter le contrat. Si l'entrepreneur souhaite embaucher un ressortissant étranger pour travailler au Canada, pour exécuter le contrat, il devrait communiquer immédiatement avec l'ambassade, le consulat ou le haut-commissariat du Canada le plus rapproché dans son pays, pour obtenir des instructions et de l'information sur les exigences de Citoyenneté et Immigration Canada et tous les documents nécessaires. L'entrepreneur doit s'assurer que les ressortissants étrangers reçoivent tous les documents, instructions et autorisations nécessaires avant d'exécuter des travaux dans le cadre du contrat au Canada. L'entrepreneur doit acquitter tous les frais occasionnés par suite de la non-conformité aux exigences en matière d'immigration.

7.19 Assurances - Aucune exigence particulière

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

7.20 Instructions d'expédition (Ministère de la Défense nationale) – Rendu au lieu de destination (DAP) Incoterms 2010

A. La livraison doit s'effectuer DAP – Rendu au lieu de destination au lieu de livraison mentionné à l'annexe A selon les Incoterms 2010. L'entrepreneur est responsable des formalités d'exportation, des frais de transport, de son administration et des risques reliés au transport. Le MDN est responsable des formalités d'importation, incluant le paiement des frais de reliés au dédouanement et des taxes

7.21 Règlement des différends

A. Les parties conviennent de maintenir une communication ouverte et honnête concernant les travaux pendant toute la durée de l'exécution du marché et après.

B. Les parties conviennent de se consulter et de collaborer dans l'exécution du marché, d'informer rapidement toute autre partie des problèmes ou des différends qui peuvent survenir et de tenter de les résoudre.

C. Si les parties n'arrivent pas à résoudre un différend au moyen de la consultation et de la collaboration, les parties conviennent de consulter un tiers neutre offrant des services de règlement extrajudiciaire des différends pour tenter de régler le problème.

D. Vous trouverez des choix de services de règlement extrajudiciaire des différends sur le site Web Achats et ventes du Canada sous le titre « Règlement des différends ».

ANNEXE « A » – ÉNONCÉ DES BESOINS

SYSTÈME DE SURVEILLANCE DE L'ENVIRONNEMENT

1. INTRODUCTION

1.1 Le ministère de la Défense nationale (MDN) a besoin d'un système de surveillance de l'environnement doté d'enregistreurs de données et d'alarmes pour contrôler de façon continue et à distance la température des réfrigérateurs entre 2 et 8 °C et des congélateurs à -20 °C et à -80 °C déployés pour l'entreposage de vaccins contre la COVID-19.

2. BIENS ET SERVICES

2.1 Besoins initiaux (de base)

L'entrepreneur doit fournir une solution permettant de contrôler, à partir d'une plateforme Web centrale, la température de quatre-vingt-seize (96) réfrigérateurs et congélateurs situés dans trente (30) sites différents au Canada (voir l'appendice 1 de l'annexe A, Emplacements des biens à surveiller).

2.1.1. Équipement

2.1.1.1 Sondes émettrices avec certificat d'étalonnage :
- 2.1.1.1.1 cinq (5) pour les congélateurs à -80 °C;
- 2.1.1.1.2 trente (30) pour les congélateurs à -20 °C;
- 2.1.1.1.3 soixante-et-une (61) pour les réfrigérateurs entre 2 °C et 8 °C.

2.1.1.2 Passerelles de réception dotées d'un routeur GSM. L'entrepreneur doit déterminer la quantité totale de passerelles de réception nécessaire en fonction de la technologie proposée et de la disposition des réfrigérateurs et des congélateurs dans chaque emplacement (voir APPENDICE 3 DE L'ANNEXE A). Il doit indiquer le nombre de passerelles requises pour chaque emplacement.

2.1.2 Abonnement (récurrent)

2.1.2.1 Progiciel pour les quatre-vingt-seize (96) sondes émettrices, sans limites du nombre d'utilisateurs et du nombre d'alarmes (téléphone, courriel ou message texte).

2.1.2.2 Forfait cellulaire pour chaque passerelle de réception, avec une quantité suffisante de données pour permettre le fonctionnement de dix (10) sondes à un intervalle d'échantillonnage de cinq (5) minutes.

2.1.3 *Services*

2.1.3.1 Une (1) séance d'instruction des opérateurs par site, pour cinq (5) à dix (10) personnes.

2.1.3.2 Une (1) séance d'instruction technique pour deux (2) à huit (8) personnes.

2.2 Besoin optionnel

2.1.2 Équipement

2.1.2.1 Sondes émettrices supplémentaires avec certificat d'étalonnage, soit jusqu'à soixante-douze (72) unités sur trois (3) ans (c.-à-d. jusqu'à vingt-quatre [24] unités par année).

2.1.2.2 Passerelles de réception supplémentaires dotées d'un routeur GSM, soit jusqu'à dix-huit (18) unités sur trois (3) ans (c.-à-d. jusqu'à six [6] unités par année).

2.2.2 *Services*

2.2.2.1 Une (1) séance d'instruction des opérateurs par site, pour cinq (5) à dix (10) personnes.
2.2.2.2 Une (1) séance d'instruction technique pour deux (2) à huit (8) personnes.
2.2.2.3 Un (1) étalonnage hors site des sondes par année, pour une période maximale de trois (3) ans.

2.2.3 *Abonnement (récurrent)*

2.2.3.1 Sondes supplémentaires pour le progiciel, soit jusqu'à soixante-douze (72) unités sur trois (3) ans (c.-à-d. jusqu'à vingt-quatre [24] unités chaque année). Prolongation de l'abonnement au progiciel, pour une période maximale de trois (3) ans.
2.2.3.2 Forfaits cellulaires supplémentaires, soit jusqu'à dix-huit (18) forfaits sur une période de trois (3) ans (c.-à-d. jusqu'à six [6] forfaits par année).
2.2.3.3 Prolongation des forfaits cellulaires, pour une période maximale de trois (3) ans.

3. CERTIFICATIONS ET NORMES

3.1 Le système de surveillance de l'environnement doit être certifié par l'Association canadienne de normalisation (CSA) ou l'équivalent (une preuve de certification ou une preuve d'équivalence doit être jointe à la soumission) [https://www.csagroup.org/fr/services-dessai-et-de-certification/marques-et-etiquettes/]. L'équivalence doit être reconnue par le Conseil canadien des normes (CCN) [https://www.scc.ca/fr].

3.2 Le système de surveillance de l'environnement doit comprendre un logiciel validé : qualification de l'installation, qualification opérationnelle et qualification de performance.

3.3 Le système de surveillance de l'environnement doit être doté d'un logiciel conforme à la partie 11, Electronic Records; Electronic Signatures – Scope and Application, du titre 21 du Code of Federal Regulations de la Food and Drug Administration.

3.4 Les sondes du système de surveillance de l'environnement doivent comprendre un certificat d'étalonnage en trois points, traçable par le National Institute of Standards and Technology (NIST) avec garantie d'erreur ne dépassant pas ±0,5 °C à chaque point d'étalonnage.

4. BESOINS EN MATÉRIEL

4.1 Le système de surveillance de l'environnement doit permettre de surveiller :

4.1.1. la température des congélateurs;
4.1.2. la température des réfrigérateurs;
4.1.3. la température ambiante;
4.1.4. l'humidité;
4.1.5. les pannes de courant;
4.1.6. les inondations.

4.2 Le système de surveillance de l'environnement doit permettre de mesurer des températures allant de -86 °C à 10 °C.

4.3 Les sondes du système de surveillance de l'environnement doivent avoir une incertitude de ±0,5 °C (±1 °F).

4.4 Le système de surveillance de l'environnement doit permettre de collecter des données et de les transférer vers une plateforme Web centrale (logiciel), le tout en temps réel. Le délai entre la température actuelle et la température enregistrée dans le logiciel doit être d'au plus une (1) heure.

4.5 Le système de surveillance de l'environnement des trente (30) sites doit être connecté au même logiciel.

4.6 Le système de surveillance de l'environnement doit être prêt à transmettre des données à la plateforme Web (logiciel) à partir d'un réseau cellulaire et d'un réseau Ethernet.

4.7 Le système de surveillance de l'environnement doit comprendre un portail sécurisé permettant d'accéder à distance aux données recueillies.

4.8 Le système de surveillance de l'environnement doit comprendre des alarmes sonores et visuelles pour chaque congélateur et réfrigérateur.

4.9 D'autres capteurs doivent pouvoir être intégrés au système de surveillance de l'environnement une fois qu'il est mis en œuvre.

4.10 Le système de surveillance de l'environnement doit pouvoir être réinstallé dans l'éventualité d'une extension future ou être installé dans des emplacements différents, tout en permettant d'accéder aux données au moyen du même logiciel.

4.11 Le système de surveillance de l'environnement doit être doté d'une batterie de secours.

5. BESOINS EN LOGICIELS

5.1 Le logiciel doit pouvoir prendre en charge un grand nombre de capteurs dans une même base de données, aux fins d'extension (plus de 1 000).

5.2 Le logiciel doit permettre d'attribuer un emplacement et un identifiant à chaque appareil.

5.3 Le logiciel doit être accessible à partir d'appareils mobiles ou d'ordinateurs personnels.

5.4 Le logiciel doit être accessible par un minimum de 100 000 utilisateurs. L'accès des utilisateurs doit être laissé à la discrétion du MDN.

5.5 Le logiciel doit permettre l'authentification des utilisateurs au moyen d'un identifiant personnel et d'un mot de passe.

5.6 Le logiciel doit permettre de créer différents profils d'utilisateur :

5.6.1 administrateur;
5.6.2 superviseur;
5.6.3 utilisateur;
5.6.4 assurance de la qualité.

5.7 Le logiciel doit permettre d'imposer des restrictions d'accès, de modification, d'ajout et de suppression à chaque profil d'utilisateur pour les paramètres suivants :

5.7.1 l'accès aux appareils;
5.7.2 les droits des utilisateurs.

5.8 Le logiciel doit permettre de configurer les appareils entièrement à distance, notamment les éléments suivants :

5.8.1 les intervalles d'échantillonnage;
5.8.2 les limites de température;
5.8.3 les alarmes;
5.8.4 la configuration des rapports.

5.9 Le logiciel doit permettre une gestion à plusieurs niveaux des alarmes, notamment :

5.9.1 un nombre illimité d'alarmes envoyées par message texte, téléphone ou courriel;
5.9.2 une transmission des alarmes à un maximum de quatre (4) personnes-ressources différentes;
5.9.3 des intervalles de transmission configurables pour les alarmes qui n'ont pas été traitées.

5.10 Le logiciel doit permettre de régler des intervalles d'échantillonnage d'au moins cinq (5) minutes.

5.11 Le logiciel doit avoir une capacité de stockage des données d'au moins douze (12) mois pour la production de rapports.

5.12 Le logiciel doit fournir l'historique des données de chaque capteur. Les données doivent pouvoir être exportées dans Microsoft Excel.

5.13 Le logiciel doit générer des rapports automatisés quotidiens, hebdomadaires et mensuels (pour chaque capteur) et un tableau des valeurs minimales et maximales enregistrées par tous les capteurs.

5.14 Les rapports générés par le logiciel ne doivent pas être modifiables.

6. BESOINS EN TECHNOLOGIE DE L'INFORMATION (TI)

6.1 <u>Sondes émettrices sans fil</u>

6.1.1 Les systèmes qui utilisent des sondes émettrices sans fil doivent :

6.1.1.1 respecter les exigences énoncées dans les cahiers des charges sur les normes radioélectriques d'ISDE. L'entrepreneur doit fournir une preuve du certificat d'approbation technique;
6.1.1.2 avoir une portée sans fil de moins de trente (30) mètres pour des raisons de sécurité;
6.1.1.3 fournir une description générale de l'utilisation prévue du spectre : bandes de fréquences prévues, nombre de canaux requis, puissance d'émission approximative et largeur de bande approximative nécessaire. L'entrepreneur doit fournir des diagrammes pour faciliter la compréhension du fonctionnement du système.

6.1.2 Sécurité de la plateforme Web
6.1.2.1 Les données doivent être traitées dans une zone d'opérations.

6.1.2.2 Le logiciel doit inclure une fonction de journal de vérification de la sécurité afin de permettre la détection des incidents.

6.1.2.3 Le logiciel doit respecter la norme minimale, à savoir la norme de chiffrement avancé AES 128 bits et le protocole Transport Layer Security 1.2 (TLS 1.2).

7. LIVRAISON

7.1 L'entrepreneur doit livrer les biens à l'adresse suivante :

Dépôt central de matériel médical
105, chemin Montgomery, bâtiment BB 104-A
Petawawa (Ontario)
K8H 2X3
Canada

8. INSTALLATION

8.1 L'entrepreneur doit fournir un soutien technique aux technologues en génie biomédical du MDN pour installer le matériel.

8.2 Les abonnements ne doivent pas être activés avant la date d'installation.

9. FORMATION

9.1 FORMATION DES OPÉRATEURS

9.1.1 À la demande du client, l'entrepreneur doit donner un cours virtuel d'instruction des opérateurs à l'intention du personnel du MDN. Au minimum, le cours de formation doit fournir au personnel du MDN les connaissances nécessaires pour parcourir les différents menus, systèmes et sous-systèmes, et suivre les procédures de dépannage de base du système. À la fin de la formation, le personnel des Services de santé des Forces canadiennes devrait pouvoir utiliser le système avec aisance.

9.1.2 L'entrepreneur doit fournir :

9.1.2.1 *Séances :* À la demande du MDN, l'entrepreneur doit donner une (1) séance d'instruction obligatoire et une (1) séance d'instruction facultative à l'intention des opérateurs dans chaque emplacement indiqué dans l'appendice 1 de l'annexe A, EMPLACEMENTS DES BIENS À SURVEILLER, comme l'indiquent les sections 2.1.3.1 et 2.2.2.1. Le nombre de participants à chaque séance doit se situer entre cinq (5) et dix (10).

9.1.2.2 *Échéancier* : La formation doit être donnée dans les soixante (60) jours suivant la livraison du système ou dès que possible à la date et à l'heure convenues par le représentant de l'entrepreneur et le responsable technique.

9.1.2.3 *Lieu :* La formation doit avoir lieu en format webinaire en direct pour les emplacements du MDN indiqués dans l'appendice 1 de l'annexe A, EMPLACEMENTS DES BIENS À SURVEILLER. Le représentant de l'entrepreneur fournira un lien de l'enregistrement de la formation au responsable technique pour utilisation par les FAC dans le cadre de futures formations.

9.1.2.4 *Langue :* La formation doit être offerte en français et en anglais, comme convenu entre le représentant de l'entrepreneur et le responsable technique, selon les webinaires offerts à chaque emplacement indiqué dans l'appendice 1 de l'annexe A, EMPLACEMENTS DES BIENS À SURVEILLER.

9.1.2.5 *Licence :* L'entrepreneur doit accorder une licence perpétuelle et irrévocable pour utiliser, reproduire et traduire les manuels, le matériel et les documents de formation et de référence.

9.1.2.6 *Documentation :* L'entrepreneur doit fournir au moins une (1) copie papier et une (1) copie électronique en format PDF du manuel d'instruction sur l'utilisation à chaque participant le premier jour du cours. Ce manuel doit être disponible en anglais et en français. Le responsable technique doit fournir à l'entrepreneur la liste des participants au plus tard cinq (5) jours avant le début du cours.

9.2 FORMATION TECHNIQUE

9.2.1 L'entrepreneur doit donner un cours d'instruction pratique sur le soutien technique aux technologues en génie biomédical du MDN. Le niveau et la portée de cette instruction doivent être les mêmes que ceux qu'offre le fabricant d'équipement d'origine (FEO) à ses techniciens sur le terrain. À la fin de l'instruction, les technologues en génie biomédical du MDN doivent pouvoir dépanner, réparer et utiliser le système avec aisance, et diagnostiquer facilement les pannes du système. Au minimum, le cours d'instruction pratique sur le soutien technique doit fournir aux technologues en génie biomédical du MDN les connaissances nécessaires pour parcourir efficacement les différents menus, systèmes et sous-systèmes, et leur donner une instruction complète sur la réparation, l'étalonnage et le dépannage du système et de ses périphériques.

9.2.2 L'entrepreneur doit fournir :

9.2.2.1 *Séances :* À la demande du MDN, l'entrepreneur doit donner une (1) séance d'instruction technique obligatoire et une (1) séance d'instruction technique facultative, comme l'indiquent les sections 2.1.3.2 et 2.2.2.2, dont le niveau et la portée sont les mêmes que ceux qu'offre le FEO à ses techniciens sur le terrain. Chaque séance de formation sur le service technique sera donnée à un groupe qui devrait compter de deux (2) à huit (8) technologues en génie biomédical.

9.2.2.2 *Échéancier :* La formation doit être donnée dans les soixante (60) jours suivant la livraison du système ou dès que possible à la date et à l'heure convenues par le représentant de l'entrepreneur et le responsable technique.

9.2.2.3 *Lieu :* La formation aura lieu au dépôt central de matériel médical de Petawawa (voir la section 7.1 pour l'adresse complète). Les frais de cours de l'entrepreneur comprendront les dépenses liées aux déplacements et à l'hébergement.

9.2.2.4 *Langue :* Tous les travaux doivent être réalisés en anglais.

9.2.2.5 *Licence :* L'entrepreneur doit accorder une licence perpétuelle et irrévocable pour utiliser, reproduire et traduire les manuels, le matériel et les documents de formation et de référence.

9.2.2.6 *Documents :* Au cours de la première journée de formation, l'entrepreneur doit fournir à chacun des participants une (1) copie du manuel d'entretien technique comportant des schémas et la liste des pièces de rechange. Le responsable technique doit fournir à l'entrepreneur la liste des technologues en génie biomédical qui assisteront à l'instruction au plus tard cinq (5) jours avant le début du cours.

10. ESSAIS D'ACCEPTATION

10.1 L'acceptation de la solution par le MDN dépend de la réussite des essais d'un échantillon représentatif de la solution à l'un des sites du MDN, soit celui d'« Halifax ». L'entrepreneur doit fournir les appareils, le logiciel et toutes les autres pièces de la solution qui seraient requises pour le site d'« Halifax ». L'échantillon représentatif de la solution doit être mis à l'essai après l'installation conformément aux exigences énoncées dans les sections 4 et 5 du présent énoncé des besoins, comme le mentionne l'APPENDICE 2 DE L'ANNEXE A – SYSTÈME DE SURVEILLANCE DE L'ENVIRONNEMENT – LISTE DE VÉRIFICATION DES ESSAIS D'ACCEPTATION.

10.2 Pour aider à mener les essais d'acceptation, l'entrepreneur doit fournir, sans frais supplémentaires pour le MDN, du personnel pour répondre aux questions techniques sur le matériel et le logiciel qui pourraient être soulevées durant les essais.

10.3 À l'achèvement des essais d'acceptation, le MDN fournira à l'entrepreneur une copie des résultats des essais d'acceptation. L'entrepreneur devra corriger tout problème relevé, et ce, sans frais supplémentaires pour le MDN.

11. SOUTIEN TECHNIQUE

11.1 L'entrepreneur doit offrir un soutien technique par téléphone du lundi au vendredi, de 8 h à 17 h (heure locale), aux emplacements indiqués à l'APPENDICE 1 DE L'ANNEXE A, EMPLACEMENTS DES BIENS À SURVEILLER.

11.2 Chaque année, l'entrepreneur doit offrir un service optionnel d'étalonnage des sondes hors site, comme l'indique la section 2.2.2.3. Un service doit être offert par rotation aux emplacements indiqués à l'APPENDICE 1 DE L'ANNEXE A, EMPLACEMENTS DES BIENS À SURVEILLER.

APPENDICE 1 DE L'ANNEXE A – EMPLACEMENTS DES BIENS À SURVEILLER

Province	Lieu	Congélateur à -80 °C	Congélateur à -20 °C	Réfrigérateur	Aménagement
Alberta	Cold Lake		1	3	APPENDICE 3 DE L'ANNEXE A
Alberta	Edmonton	1	1	2	APPENDICE 3 DE L'ANNEXE A
Alberta	Suffield		1	1	Congélateur et réfrigérateur installés dans la même pièce
Alberta	Wainwright		1	2	APPENDICE 3 DE L'ANNEXE A
Colombie-Britannique	Comox		1	1	Congélateur et réfrigérateur installés dans la même pièce et espacés de deux (2) pieds
Colombie-Britannique	Esquilmat	1	1	3	APPENDICE 3 DE L'ANNEXE A
Colombie-Britannique	Vancouver		1	1	APPENDICE 3 DE L'ANNEXE A
Manitoba	Shilo		1	4	APPENDICE 3 DE L'ANNEXE A
Manitoba	Winnipeg		1	2	APPENDICE 3 DE L'ANNEXE A
Nouveau-Brunswick	Gagetown		1	3	APPENDICE 3 DE L'ANNEXE A
Terre-Neuve-et-Labrador	Gander		1	1	Congélateur et réfrigérateur installés dans la même pièce
Terre-Neuve-et-Labrador	Goose Bay		1	1	APPENDICE 3 DE L'ANNEXE A
Terre-Neuve-et-Labrador	St-John's		1	1	APPENDICE 3 DE L'ANNEXE A
Territoires du Nord-Ouest	Yellowknife		1	1	Congélateur et réfrigérateur installés dans la même pièce
Nouvelle-Écosse	Greenwood		1	1	Congélateur et réfrigérateur installés dans la même pièce
Nouvelle-Écosse	Halifax	1	1	1	APPENDICE 3 DE L'ANNEXE A
Ontario	Borden		1	3	APPENDICE 3 DE L'ANNEXE A
Ontario	Kingston		1	6	APPENDICE 3 DE L'ANNEXE A
Ontario	Meaford		1	2	Congélateur et réfrigérateurs installés dans la même pièce
Ontario	North Bay		1	1	Congélateur et réfrigérateur installés dans la même pièce
Ontario	Ottawa		1	6	APPENDICE 3 DE L'ANNEXE A
Ontario	Petawawa		1	1	Congélateur et réfrigérateur installés dans la même pièce et espacés d'un (1) pied
Ontario	Toronto		1	1	Congélateur et réfrigérateur installés dans la même pièce
Ontario	Trenton		1	4	APPENDICE 3 DE L'ANNEXE A
Québec	Bagotville		1	1	Congélateur et réfrigérateur installés dans la même pièce
Québec	Montréal		1	2	APPENDICE 3 DE L'ANNEXE A
Québec	Saint-Jean	1	1	3	

Québec	Valcartier	1	1	1	APPENDICE 3 DE L'ANNEXE A
Saskatchewan	Dundurn		1	1	APPENDICE 3 DE L'ANNEXE A
Saskatchewan	Moose Jaw		1	1	Congélateur et réfrigérateur installés dans la même pièce et espacés de cinq (5) pieds
	TOTAL	**5**	**30**	**61**	

APPENDICE 2 DE L'ANNEXE A – SYSTÈME DE SURVEILLANCE DE L'ENVIRONNEMENT – LISTE DE VÉRIFICATION DES ESSAIS D'ACCEPTATION

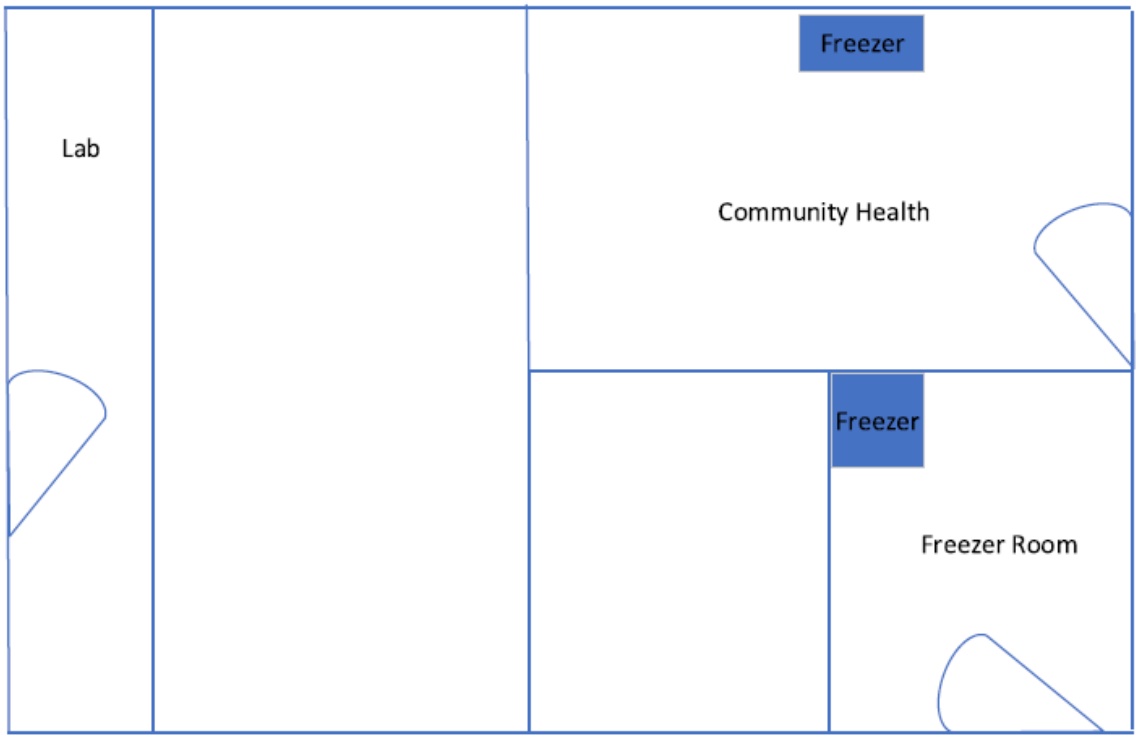
APPENDICE 2 – SYSTÈME DE SURVEILLANCE DE L'ENVIRONNEMENT – LISTE DE VÉRIFICATION DES ESSAIS D'ACCEPTATION

N° d'essai	Système de surveillance de l'environnement : fonctions à essayer	Moyen de conformité	Réussite	Échec	Commentaires
E1	5.3 Le logiciel doit être accessible à partir d'appareils mobiles ou d'ordinateurs personnels.	Une de ces deux (2) options : 1 – Lien Web du logiciel 2 – Application de bureau et application mobile			
E2	5.5 Le logiciel doit permettre l'authentification des utilisateurs au moyen d'un identifiant personnel et d'un mot de passe.	Obtenir l'identificateur d'utilisateur et le mot de passe administrateur de l'entrepreneur. Ouvrir une session administrateur avec l'identificateur et le mot de passe. Créer quatre (4) autres comptes avec le compte administrateur. Ouvrir une session avec ces quatre (4) comptes à l'aide des identificateurs et des mots de passe créés.			
E3	5.6 Le logiciel doit permettre de créer différents profils d'utilisateur : 5.6.1 Administrateur 5.6.2 Superviseur 5.6.3 Utilisateur 5.6.4 Assurance de la qualité	Banc d'essai du logiciel à partir du compte administrateur : Créer un profil de superviseur et y attribuer deux (2) comptes créés dans le cadre de l'essai 2 (ci-après les comptes S1 et S2). Créer un profil utilisateur et y attribuer les deux (2) autres comptes créés dans le cadre de l'essai 2 (ci-après les comptes U1 et U2). Créer un profil d'assurance de la qualité.			
E4	4.5 Le système de surveillance de l'environnement des trente (30) sites doit être connecté au même logiciel.	Banc d'essai du logiciel à partir du compte administrateur : Créer trente (30) sites sur le logiciel (en appeler un L1 et l'autre L2).			
E5	5.2 Le logiciel doit permettre d'attribuer un emplacement et un identifiant à chaque appareil.	Banc d'essai du logiciel à partir du compte administrateur : Connecter deux (2) nouvelles sondes émettrices au logiciel. Elles doivent être détectées par le logiciel et visibles sur la liste des appareils. Attribuer des identificateurs aux appareils (ci-après P1 et P2). Attribuer deux (2) emplacements différents aux appareils parmi les trente (30) sites (P1 est maintenant situé à l'emplacement L1 et P2 à l'emplacement L2).			
E6	5.7 Le logiciel doit permettre d'imposer des restrictions d'accès, de modification, d'ajout et de suppression à chaque profil d'utilisateur pour les paramètres suivants : 5.7.1 Accès aux appareils 5.7.2 Droits des utilisateurs	Banc d'essai du logiciel à partir du compte administrateur : Administrateur : doit être capable de visualiser, de modifier, d'ajouter et de supprimer pour chaque emplacement, c'est-à-dire P1 et P2. Attribuer L1 comme emplacement des comptes S1 et U1. S1 : doit être capable de visualiser, de modifier, d'ajouter et de supprimer pour son emplacement, c'est-à-dire P1. U1 : doit être capable de visualiser chaque appareil de son emplacement, c'est-à-dire P1. Attribuer L2 comme emplacement des comptes S2 et U2 S2 : doit être capable de visualiser, de modifier, d'ajouter et de supprimer pour son emplacement, c'est-à-dire P2. U2 : doit être capable de visualiser chaque appareil de son emplacement, c'est-à-dire P2.			
E7	5.8 Le logiciel doit permettre de configurer les appareils entièrement à distance, notamment les éléments suivants : 5.8.1 Intervalles d'échantillonnage 5.8.2 Limites de température 5.8.3 Alarmes 5.8.4 Configuration des rapports	Banc d'essai du logiciel pour un appareil (par exemple, P1) : Configurer le temps d'échantillonnage à cinq (5) minutes. Configurer les limites de température de -25 à 15 pour le congélateur et de 2 à 8 pour le réfrigérateur. Créer un rapport à partir du début (au moins 24 heures).			
E8	5.9 Le logiciel doit permettre une gestion à plusieurs niveaux des alarmes, notamment : 5.9.1 Nombre illimité d'alarmes envoyées par message texte, téléphone ou courriel 5.9.2 Transmission des alarmes à un maximum de quatre (4) personnes-ressources différentes 5.9.3 Intervalles de transmission configurables pour les alarmes qui n'ont pas été traitées	Banc d'essai du logiciel à partir du compte de superviseur (par exemple, S1) : Préciser U1 comme personne-ressource principale pour la réception des alarmes. Préciser le message texte et le courriel comme méthodes d'envoi des alarmes. Préciser la fréquence des alarmes à une (1) minute. Configurer la température à l'extérieur de la fourchette et vérifier si les alarmes sont bien envoyées.			
E9	4.8 Le système de surveillance de l'environnement doit comprendre des alarmes sonores et visuelles pour chaque congélateur et réfrigérateur.	Configurer la température à l'extérieur de la fourchette et vérifier si les alarmes visuelles et sonores sont déclenchées sur l'appareil.			
E10	4.4 Le système de surveillance de l'environnement doit permettre de collecter des données et de les transférer vers une plateforme Web centrale (logiciel), le tout en temps réel. Le délai entre la température actuelle et la température enregistrée dans le logiciel doit être d'au plus une (1) heure.	Banc d'essai du logiciel à partir du compte de superviseur (par exemple, S1) : Les températures avec les dates et les heures sont signalées dans le logiciel pour P1 en moins d'une (1) heure.			
E11	5.12 Le logiciel doit fournir l'historique des données de chaque capteur. Les données doivent pouvoir être exportées dans Microsoft Excel.	Banc d'essai du logiciel à partir du compte utilisateur (par exemple, U1) : Vérifier dans le logiciel si l'historique des températures est disponible pour P1. Exporter les données dans Microsoft Excel.			

APPENDICE 3 DE L'ANNEXE A – DISPOSITION DES RÉFRIGÉRATEURS ET DES CONGÉLATEURS PAR EMPLACEMENT

Légende
Clinique Principale de Kingston / Kingston - Main Clinic
Santé communautaire / Community Health
Congélateur / Freezer
Salle de congélation /Freezer Room
Laboratoire/Lab

Kingston - Main Clinic



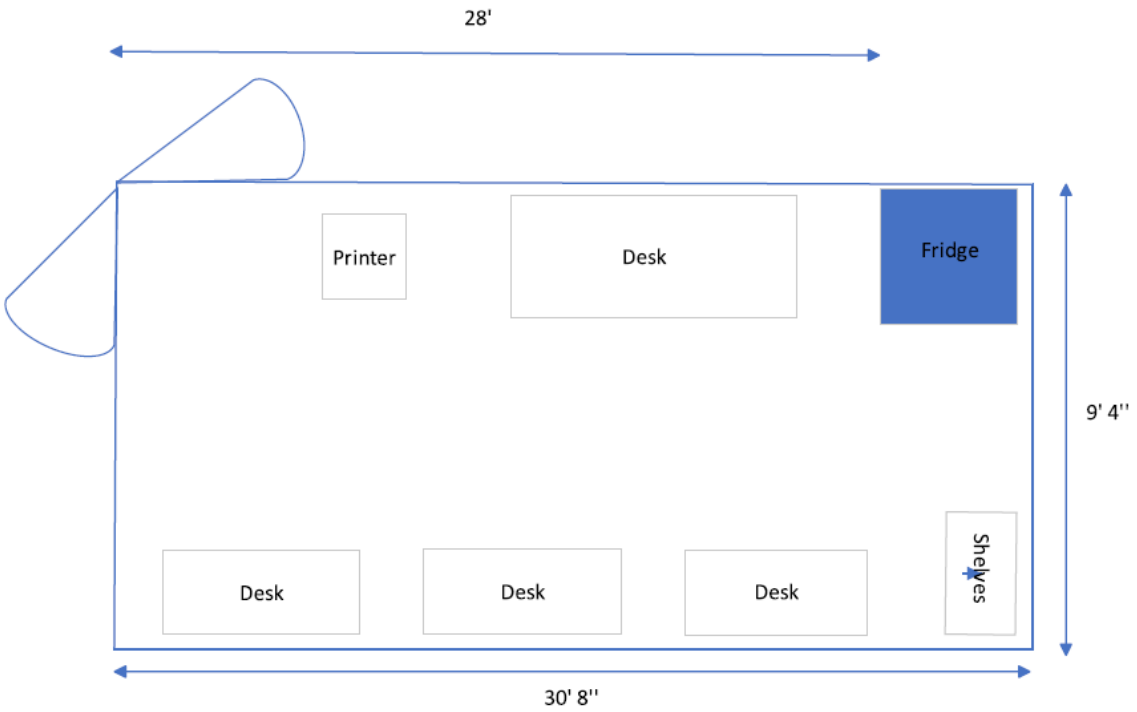
National Defence | Défense nationale

National Defence Headquarters
Ottawa, Ontario
K1A 0K2

Quartier général de la Défense nationale
Ottawa (Ontario)
K1A 0K2

Légende
Kingston - Pharmacie /Kingston - Pharmacy
Réfrigérateur / Refrigerator (Fridge)
Imprimante / Printer
Bureau / Desk
Étagères / Shelves

Kingston - Pharmacy

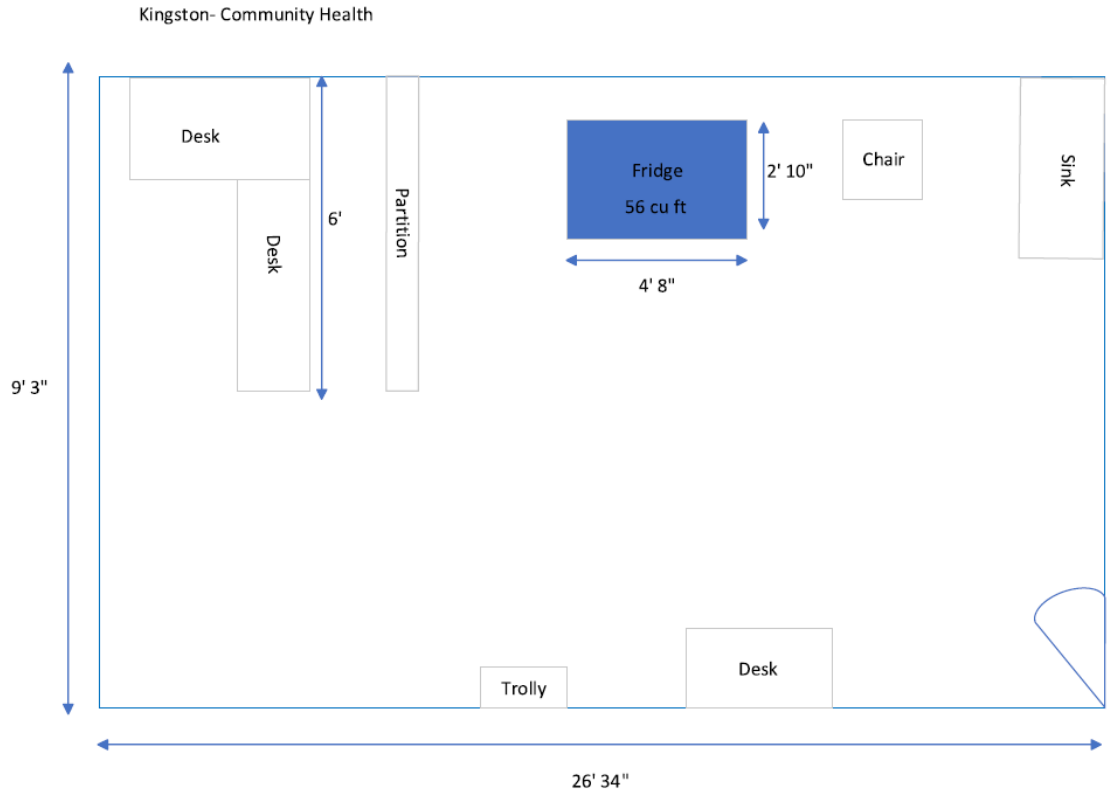


National Defence | Défense nationale

National Defence Headquarters
Ottawa, Ontario
K1A 0K2

Quartier général de la Défense nationale
Ottawa (Ontario)
K1A 0K2

Légende
Kingston - Santé communautaire /Kingston – Community Health
Réfrigérateur / Refrigerator (Fridge)
Évier / Sink
Bureau / Desk
Chaise / Chair



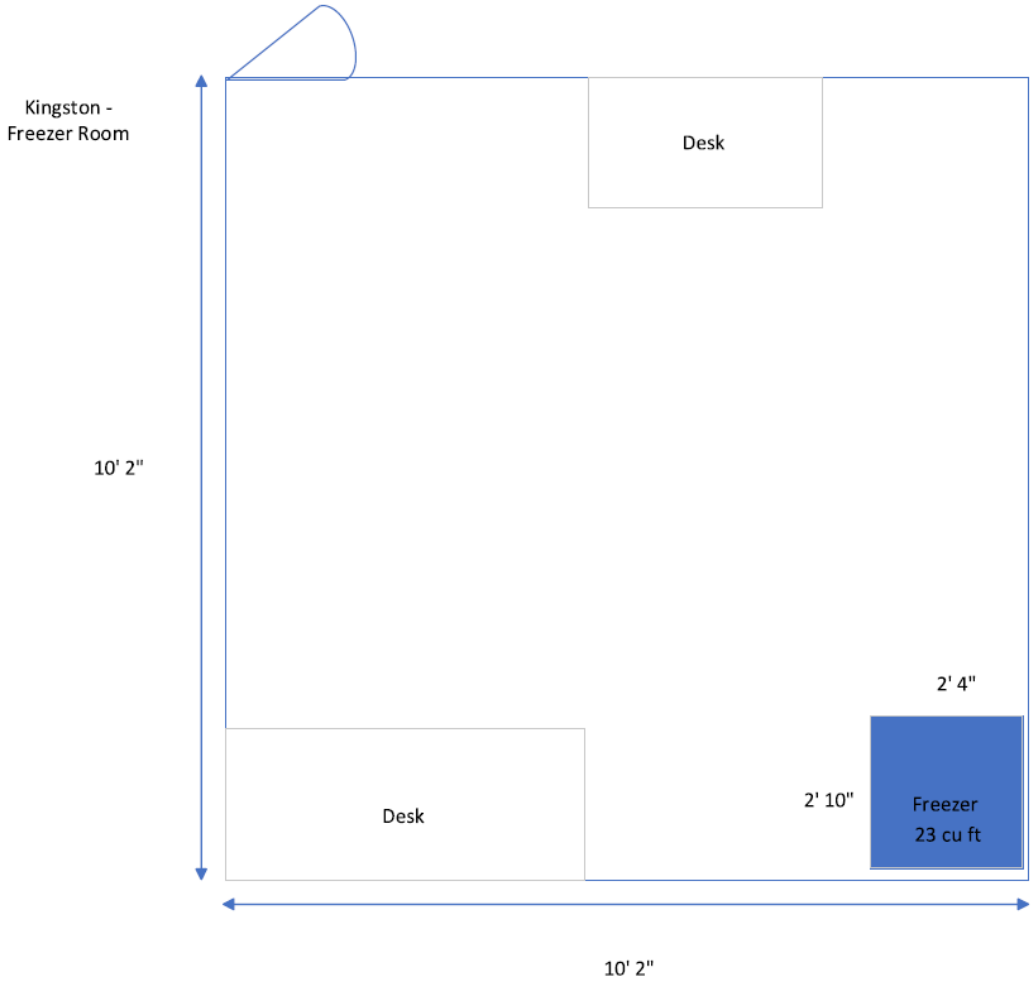
National Defence

National Defence Headquarters
Ottawa, Ontario
K1A 0K2

Défense nationale

Quartier général de la Défense nationale
Ottawa (Ontario)
K1A 0K2

Légende
Kingston - Salle de congélation /Kingston – Freezer Room
Bureau / Desk
Congélateur / Freezer
pieds cube (pi³) /cu ft



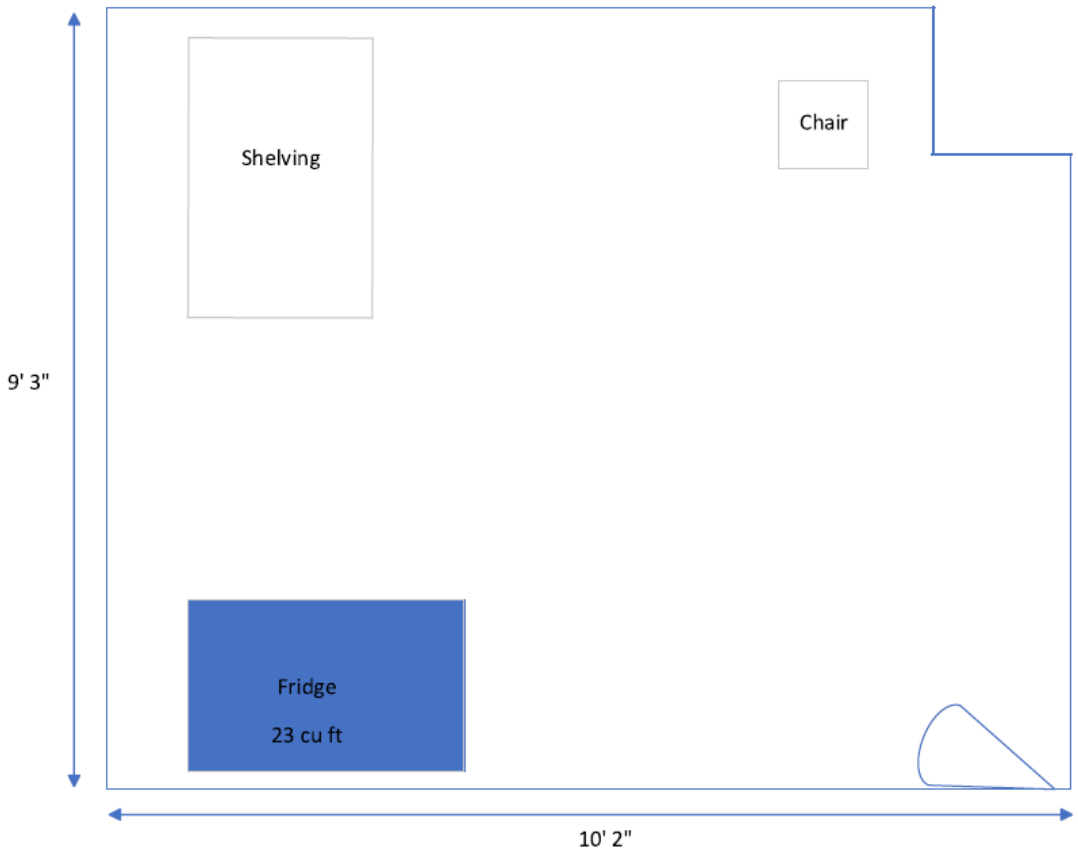
National Defence | Défense nationale

National Defence Headquarters
Ottawa, Ontario
K1A 0K2

Quartier général de la Défense nationale
Ottawa (Ontario)
K1A 0K2

Légende
Kingston – Chambre froide de laboratoire /Kingston – Lab Cold Room
Réfrigérateur / Refrigerator (Fridge)
Étagères / Shelves (Shelving)
Chaise / Chair
pieds cube (pi³) /cu ft

Kingston - Lab Cold Room

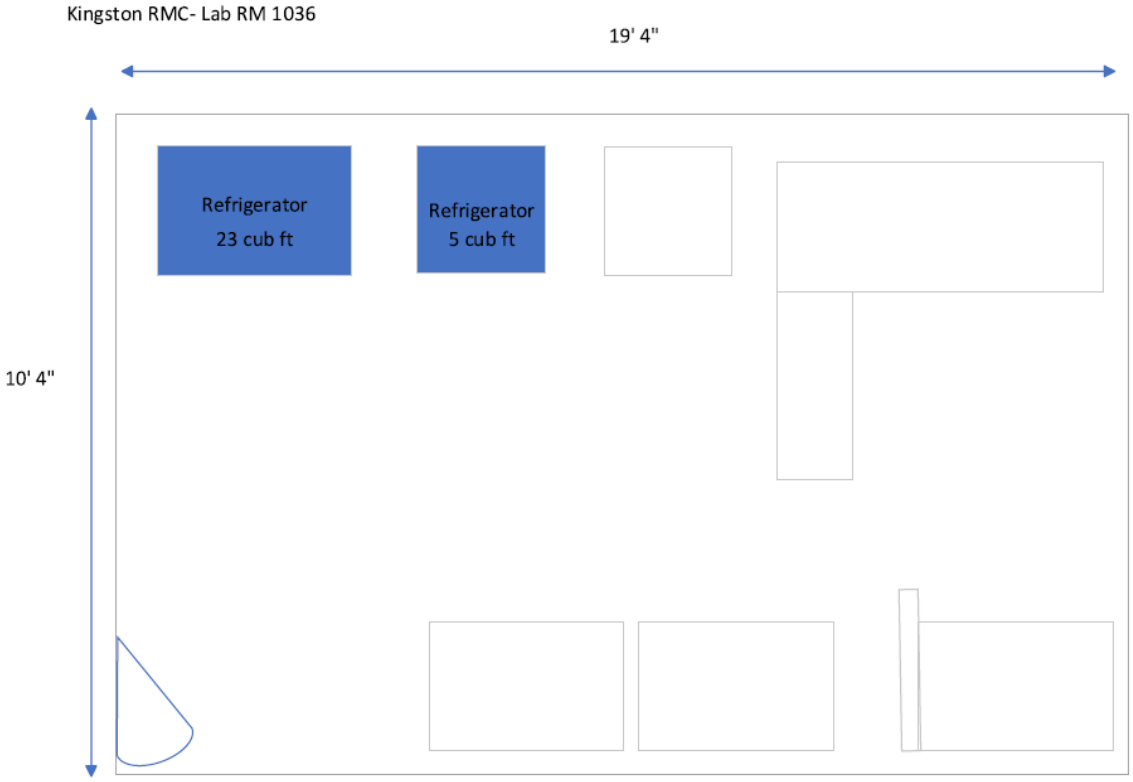


National Defence | Défense nationale

National Defence Headquarters
Ottawa, Ontario
K1A 0K2

Quartier général de la Défense nationale
Ottawa (Ontario)
K1A 0K2

Légende
Kingston – CMR – Laboratoire RM 1036 /Kingston – RMC – Lab RM 1036
Réfrigérateur / Refrigerator
pieds cube (pi³) /cu ft

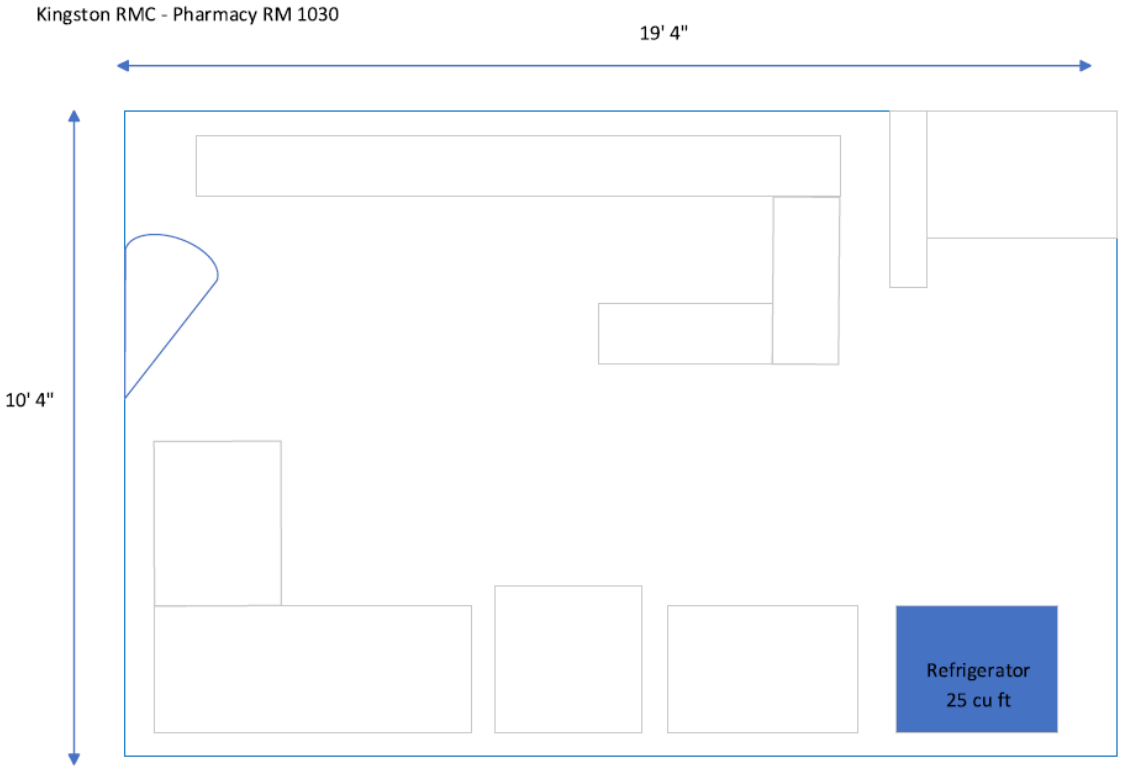


National Defence | Défense nationale

National Defence Headquarters
Ottawa, Ontario
K1A 0K2

Quartier général de la Défense nationale
Ottawa (Ontario)
K1A 0K2

Légende
Kingston CMR – Pharmacie RM 1030 /Kingston RMC – Pharmacy RM 1030
Réfrigérateur / Refrigerator
pieds cube (pi³) /cu ft



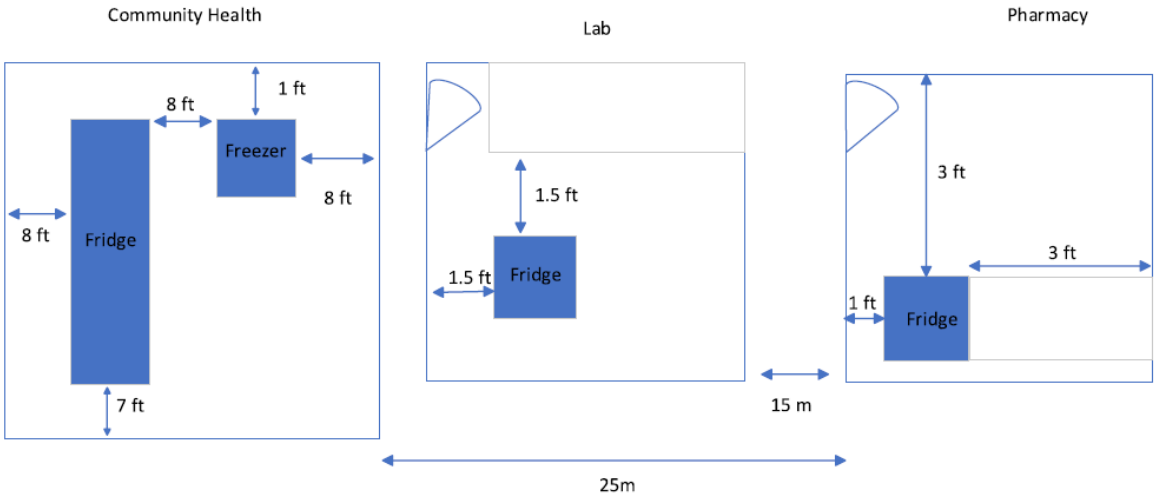
National Defence | Défense nationale

National Defence Headquarters
Ottawa, Ontario
K1A 0K2

Quartier général de la Défense nationale
Ottawa (Ontario)
K1A 0K2

Légende
Santé communautaire /Community Health
Laboratoire /Lab
Pharmacie /Pharmacy
Réfrigérateur / Refrigerator (Fridge)
Congélateur / Freezer
pi /ft

Borden

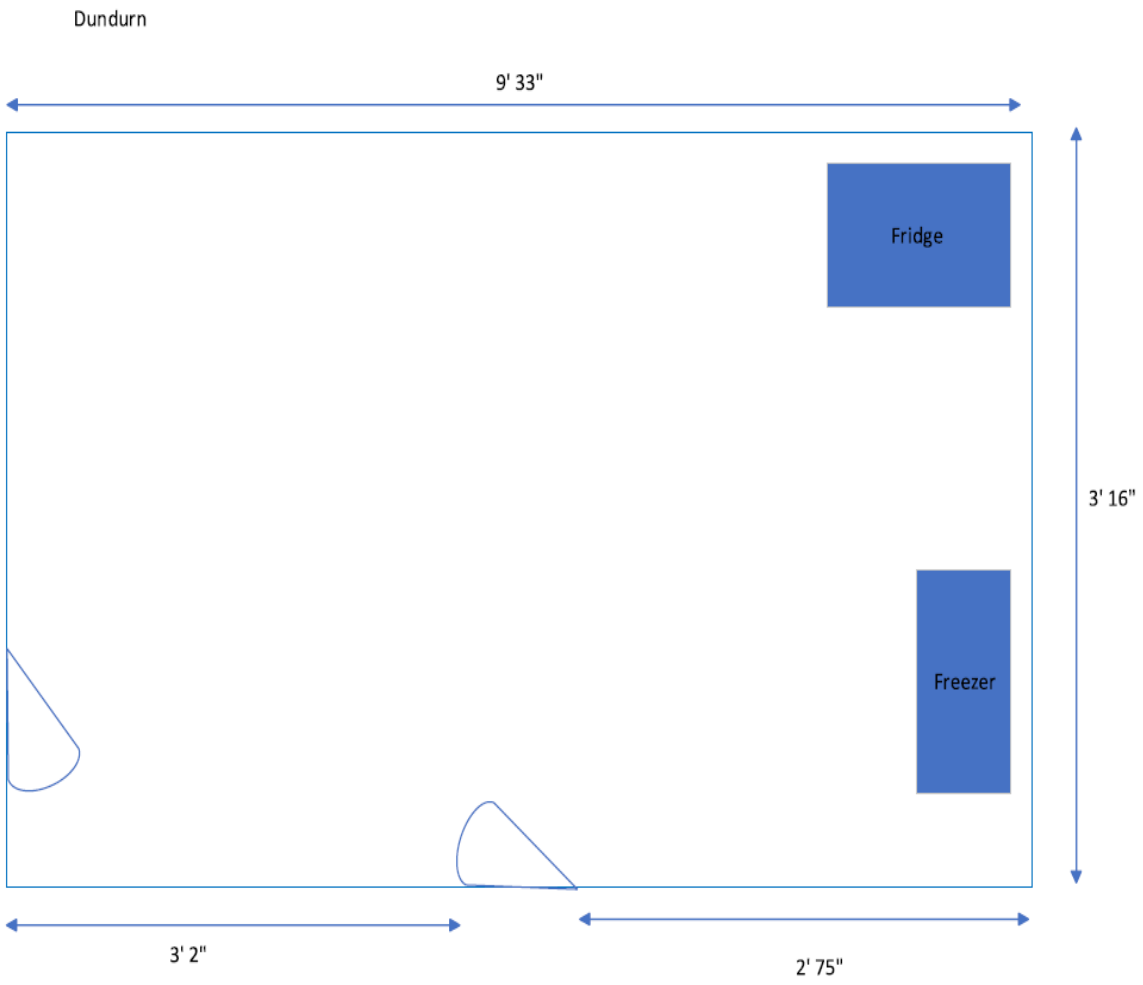


National Defence | Défense nationale

National Defence Headquarters
Ottawa, Ontario
K1A 0K2

Quartier général de la Défense nationale
Ottawa (Ontario)
K1A 0K2

Légende
Réfrigérateur / Refrigerator (Fridge)
Congélateur / Freezer



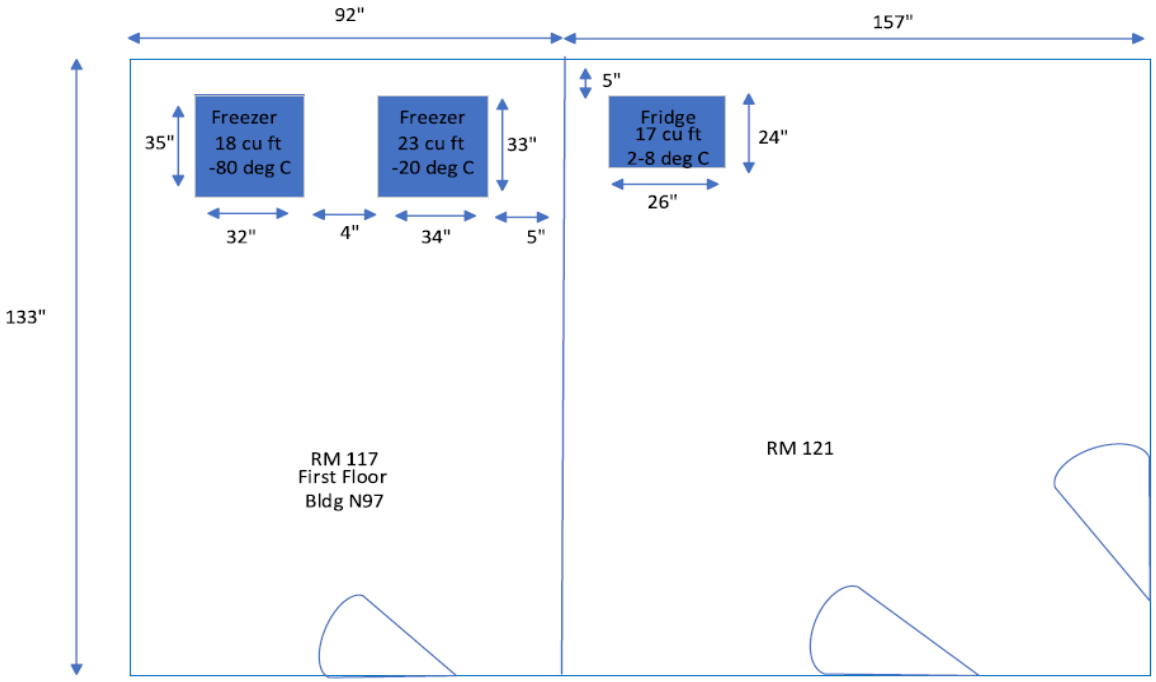
National Defence | Défense nationale

National Defence Headquarters
Ottawa, Ontario
K1A 0K2

Quartier général de la Défense nationale
Ottawa (Ontario)
K1A 0K2

Légende
Chambre /Room (RM)
Réfrigérateur / Refrigerator (Fridge)
Congélateur / Freezer
Premier étage du bâtiment / First Floor Bldg
Degré C / Deg C
pieds cube (pi³) /cu ft

Esquimalt - Room 117 & 121



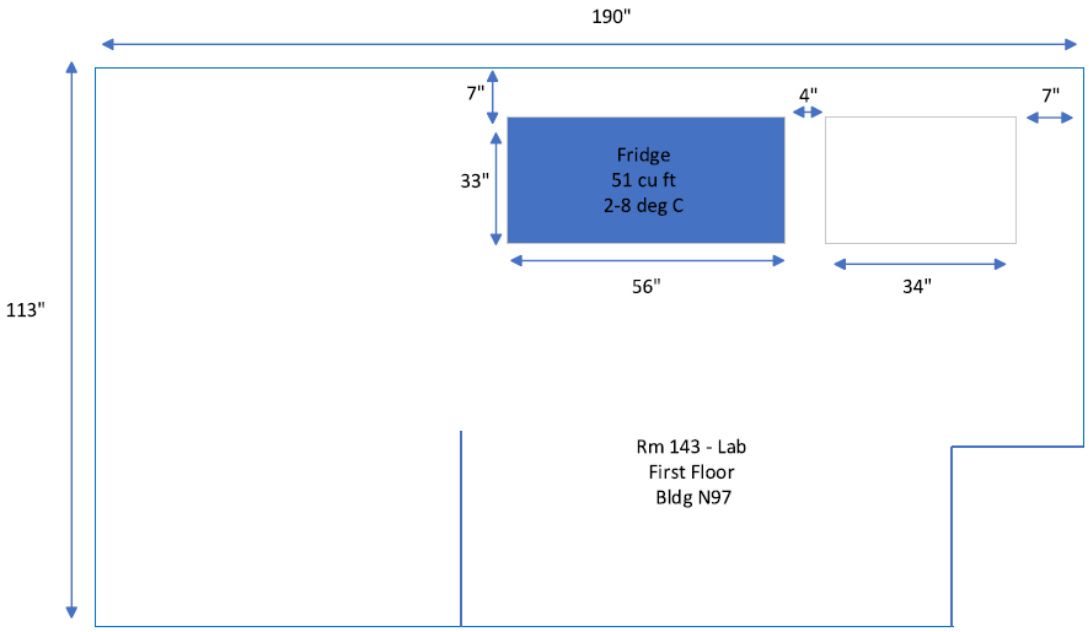
National Defence | Défense nationale

National Defence Headquarters
Ottawa, Ontario
K1A 0K2

Quartier général de la Défense nationale
Ottawa (Ontario)
K1A 0K2

Légende
Chambre /Room (RM)
Réfrigérateur / Refrigerator (Fridge)
Premier étage du bâtiment /First Floor Bldg
Degré C / Deg C
pieds cube (pi³) /cu ft

Esquimalt - Room 143

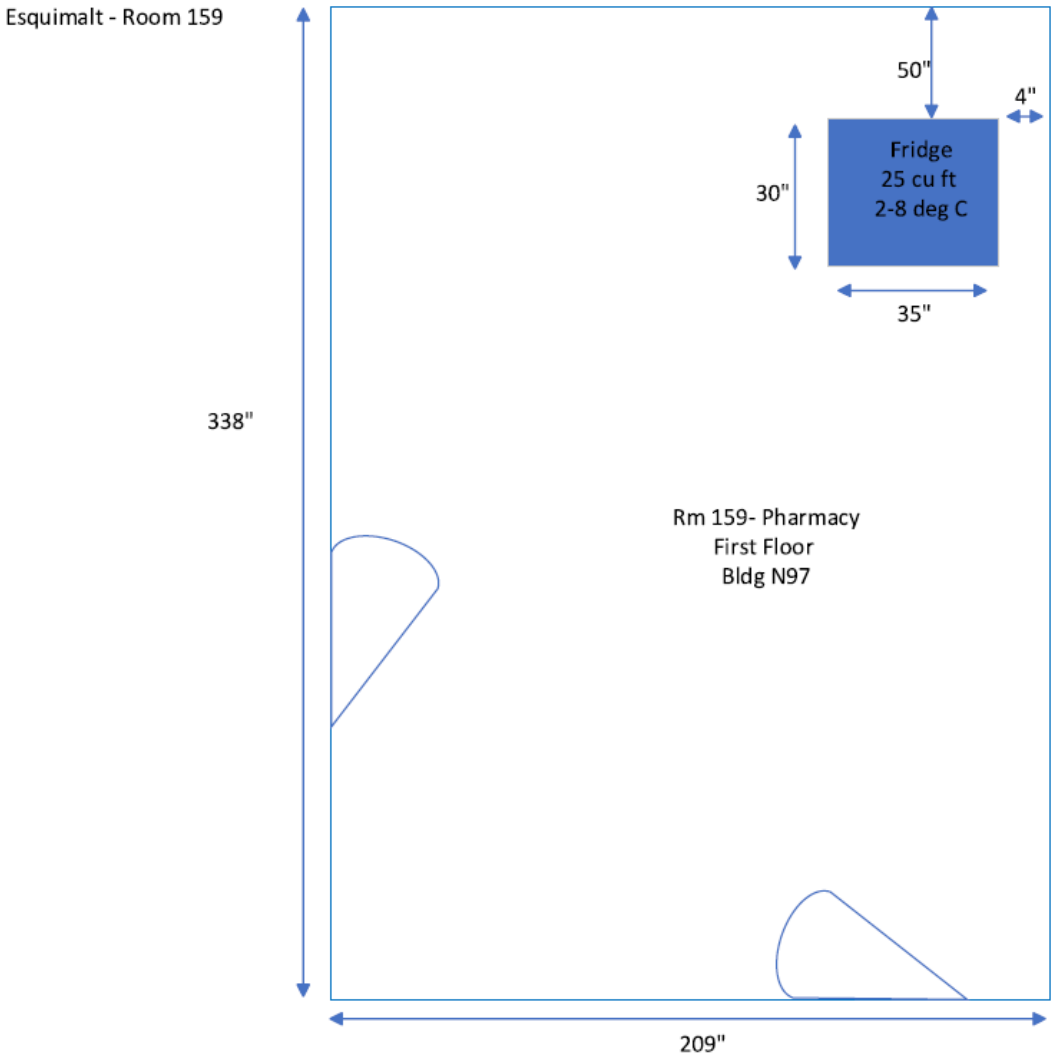


National Defence | Défense nationale

National Defence Headquarters
Ottawa, Ontario
K1A 0K2

Quartier général de la Défense nationale
Ottawa (Ontario)
K1A 0K2

Légende
Salle 159 de Pharmacie /Room (RM) 159 Pharmacy
Réfrigérateur / Refrigerator (Fridge)
Premier étage du bâtiment /First Floor Bldg
Degré C / Deg C
pieds cube (pi³) /cu ft

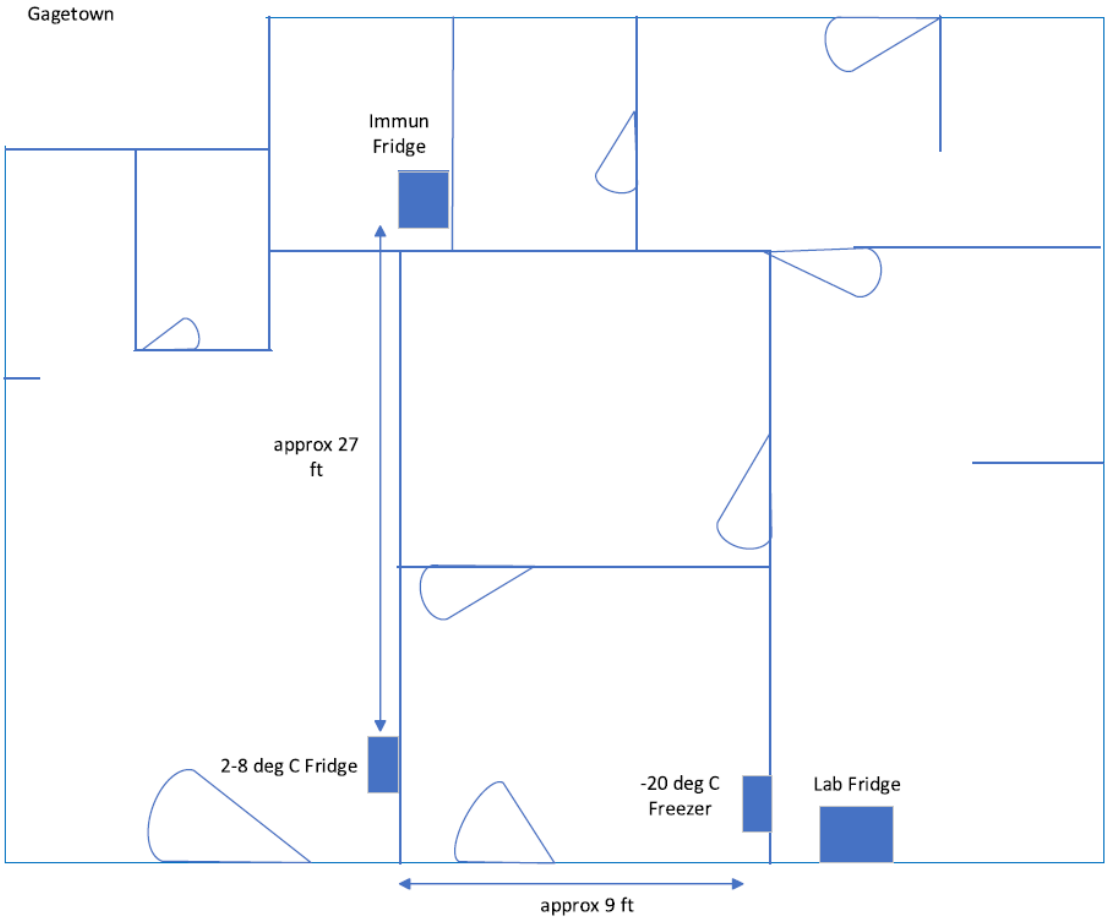


National Defence | Défense nationale

National Defence Headquarters
Ottawa, Ontario
K1A 0K2

Quartier général de la Défense nationale
Ottawa (Ontario)
K1A 0K2

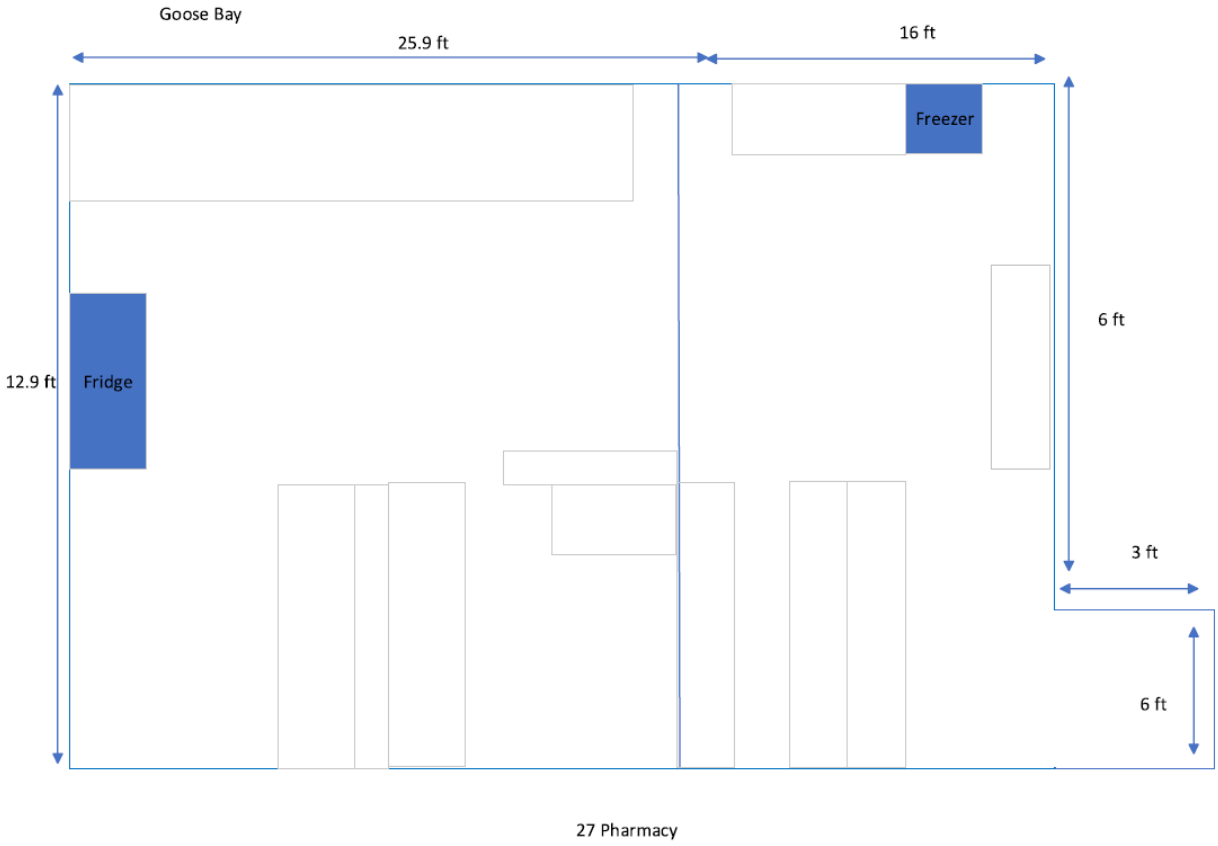
Légende
Réfrigérateur de vaccination / Immun Fridge
Réfrigérateur / Refrigerator (Fridge)
Premier étage du bâtiment /First Floor Bldg
Degré C / Deg C
pieds cube (pi³) /cu ft
Congélateur / Freezer



National Defence
National Defence Headquarters
Ottawa, Ontario
K1A 0K2

Défense nationale
Quartier général de la Défense nationale
Ottawa (Ontario)
K1A 0K2

Légende
Congélateur / Freezer
Réfrigérateur / Refrigerator (Fridge)
pi /ft

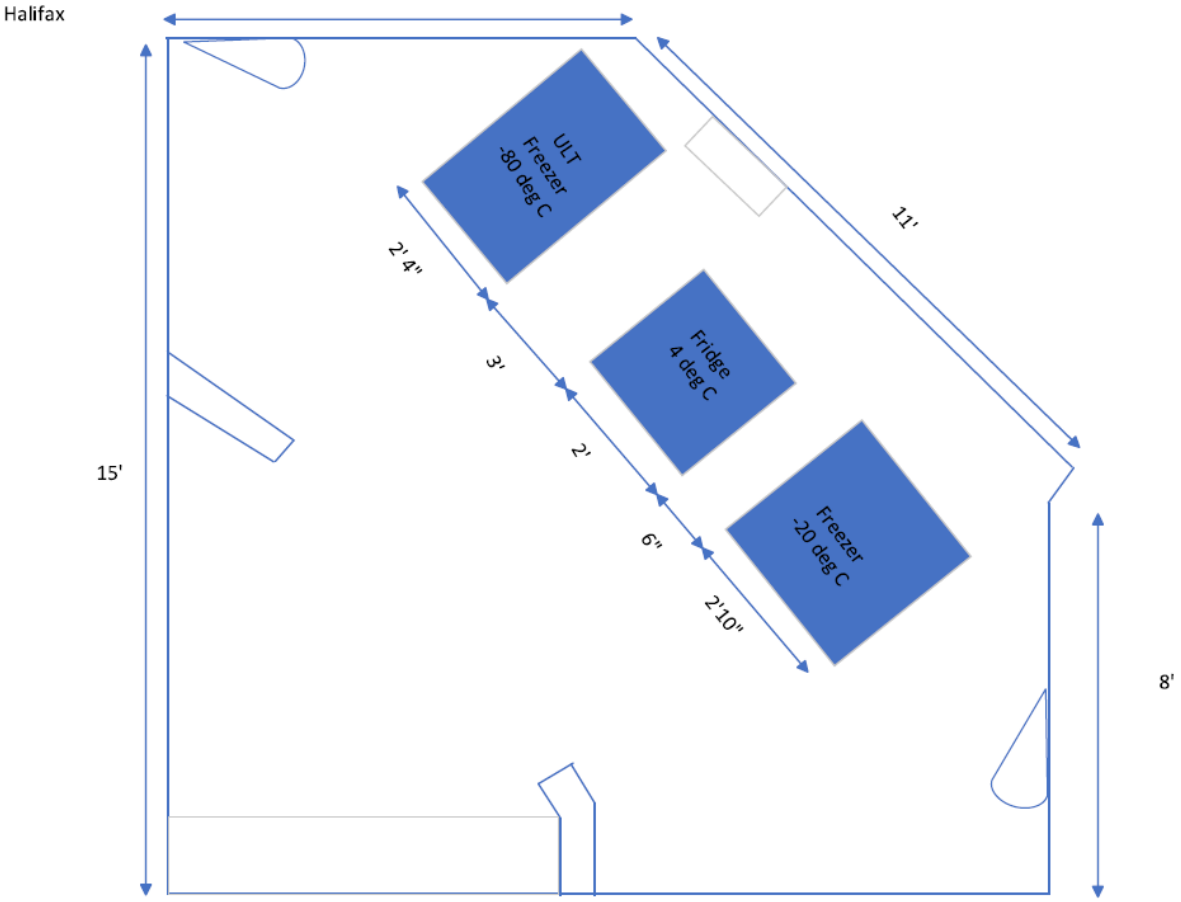


National Defence | Défense nationale

National Defence Headquarters
Ottawa, Ontario
K1A 0K2

Quartier général de la Défense nationale
Ottawa (Ontario)
K1A 0K2

Légende
Congélateur / Freezer
Réfrigérateur / Refrigerator (Fridge)
Degré C /deg C



National Defence | Défense nationale

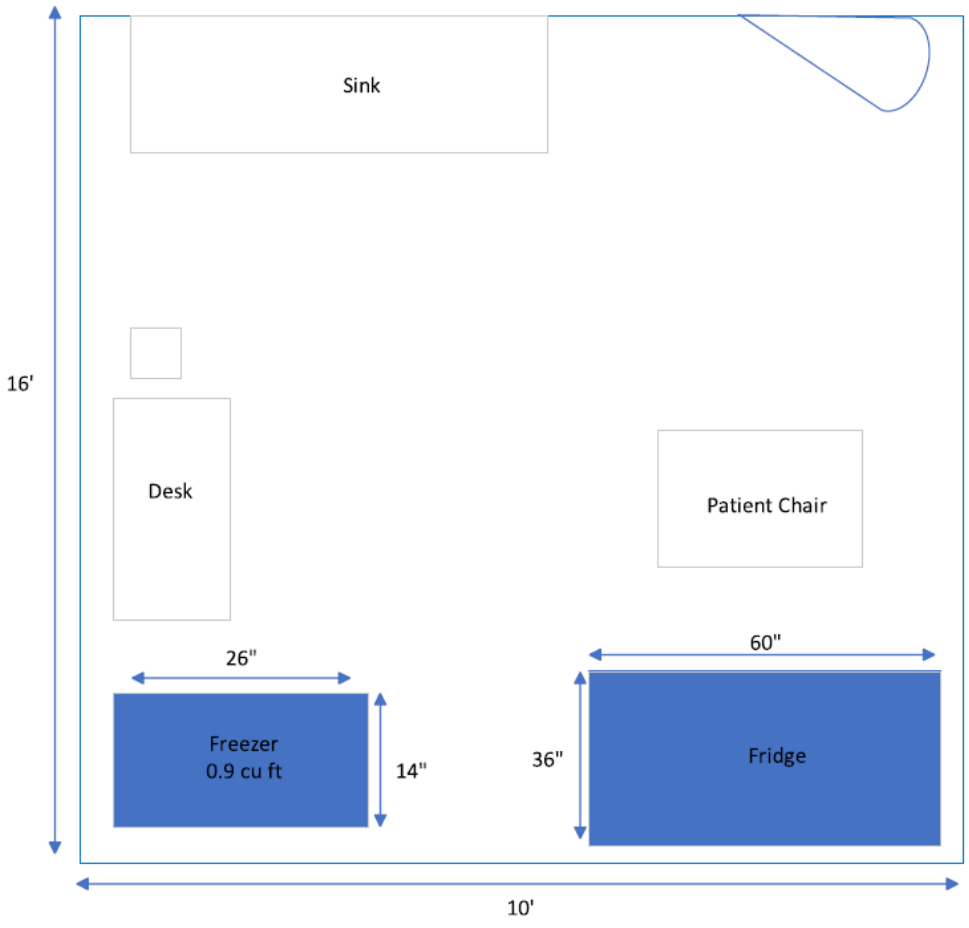
National Defence Headquarters
Ottawa, Ontario
K1A 0K2

Quartier général de la Défense nationale
Ottawa (Ontario)
K1A 0K2

Légende
Salle de vaccination /Immunization Room
Congélateur / Freezer
Réfrigérateur / Refrigerator
Chaise du patient / Patient Chair
Évier / Sink
Bureau / Desk
pieds cube (pi³) /cu ft

Longue-Pointe

Immunization Room- Longue-Pointe- Montreal

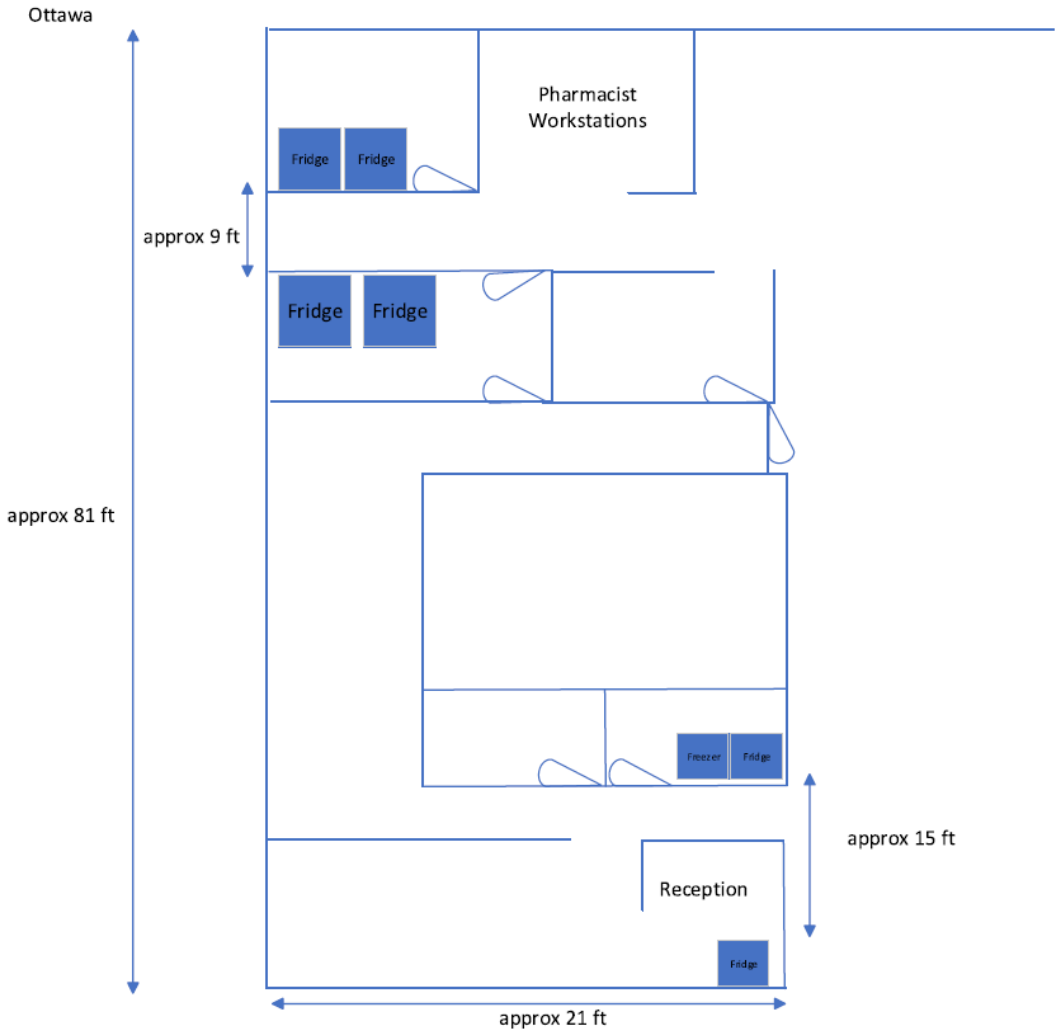


National Defence | Défense nationale

National Defence Headquarters
Ottawa, Ontario
K1A 0K2

Quartier général de la Défense nationale
Ottawa (Ontario)
K1A 0K2

Légende
Postes Pharmacien / Pharmacist Workstations
Congélateur / Freezer
Réfrigérateur / Refrigerator (Fridge)
Environ / Approx
Réception / Reception
pi /ft

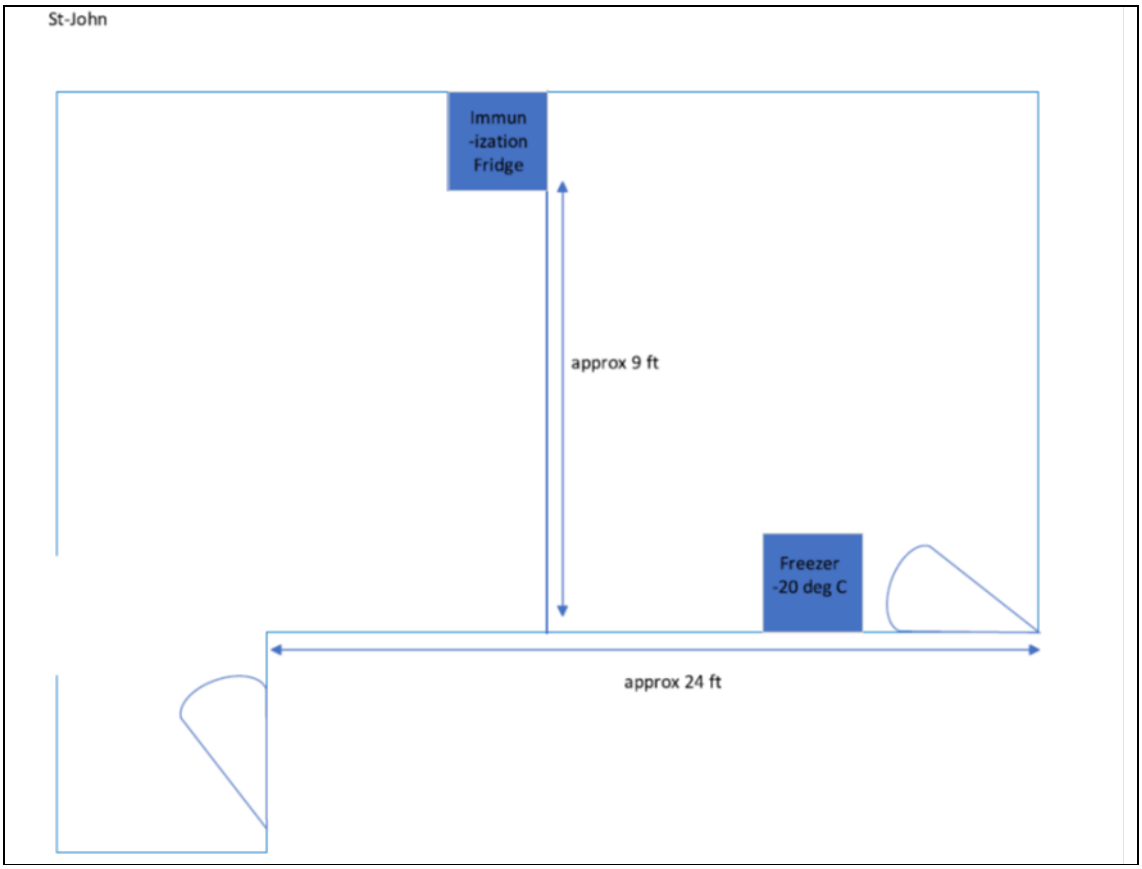


National Defence | Défense nationale

National Defence Headquarters
Ottawa, Ontario
K1A 0K2

Quartier général de la Défense nationale
Ottawa (Ontario)
K1A 0K2

Légende
Réfrigérateur de vaccination / Immunization Fridge
Congélateur / Freezer
pi / ft
Environ / Approx
Degré C / deg C



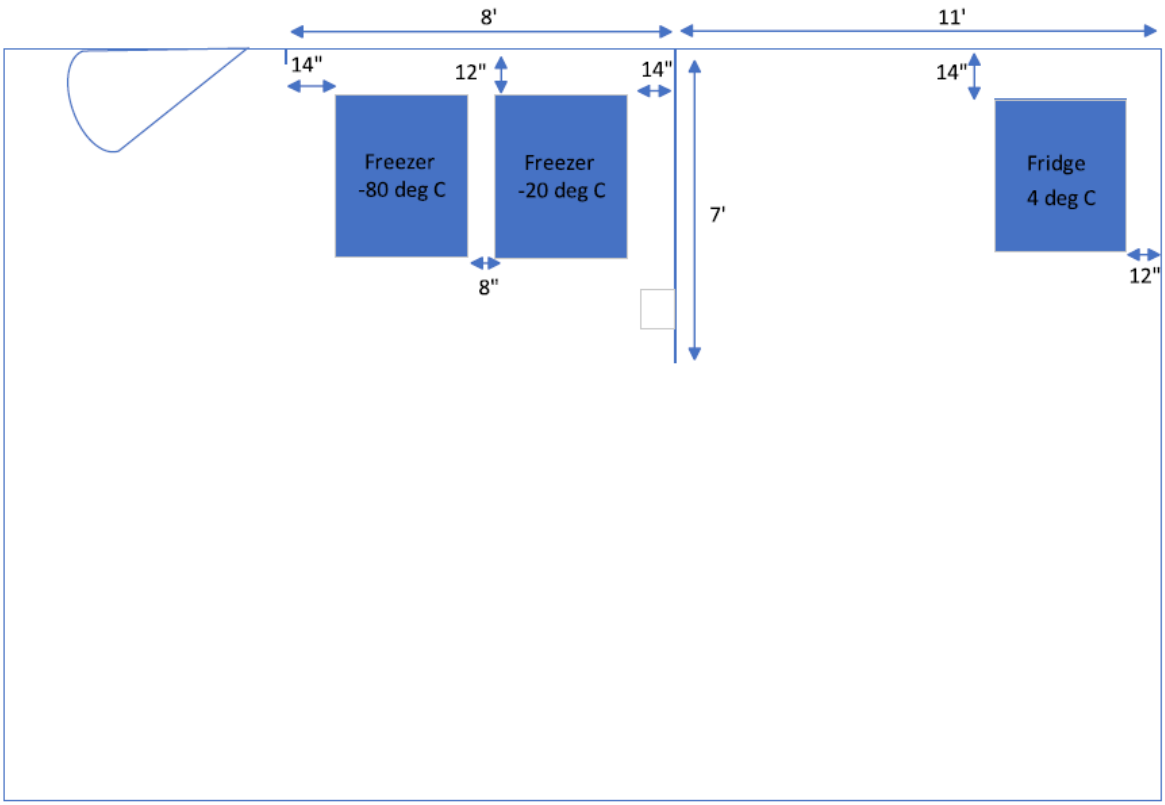
National Defence | Défense nationale

National Defence Headquarters
Ottawa, Ontario
K1A 0K2

Quartier général de la Défense nationale
Ottawa (Ontario)
K1A 0K2

Légende
Congélateur / Freezer
Réfrigérateur / Refrigerator

Valcartier



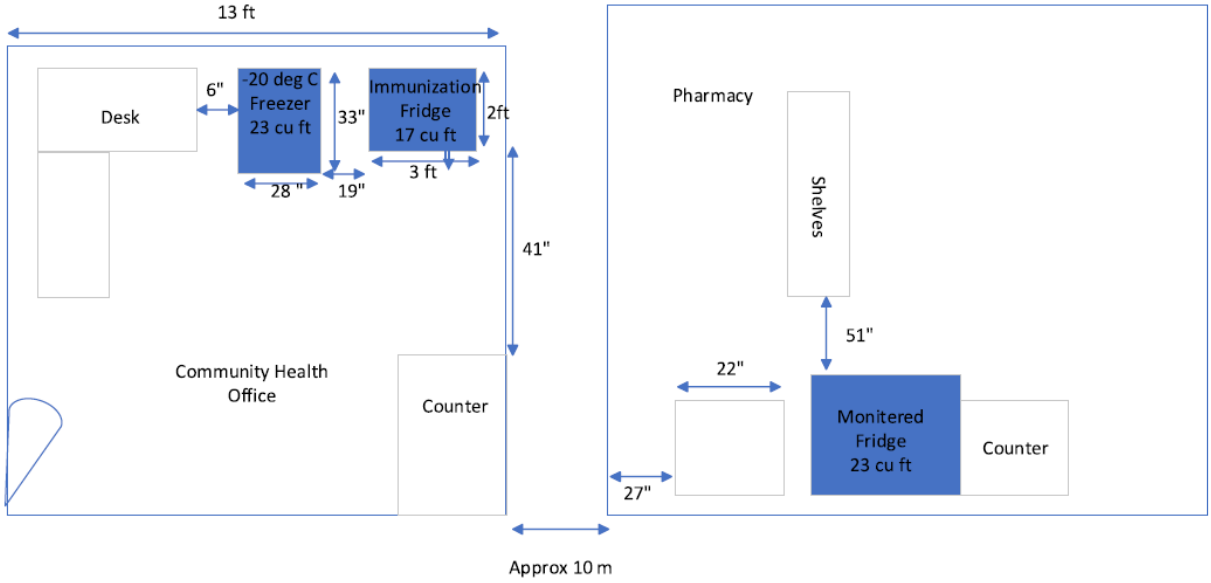
National Defence | Défense nationale

National Defence Headquarters
Ottawa, Ontario
K1A 0K2

Quartier général de la Défense nationale
Ottawa (Ontario)
K1A 0K2

Légende
Bureau de santé communautaire / Community Health Office
Pharmacie / Pharmacy
Congélateur / Freezer
Bureau / Desk
Réfrigérateur surveillé / Monitored Fridge
Comptoir / Counter
Étagères / Shelves
Réfrigérateur de vaccination / Immunization Fridge
pieds cube (pi³) /cu ft
Degré C / deg C
Environ / Approx

Wainright



National Defence | Défense nationale

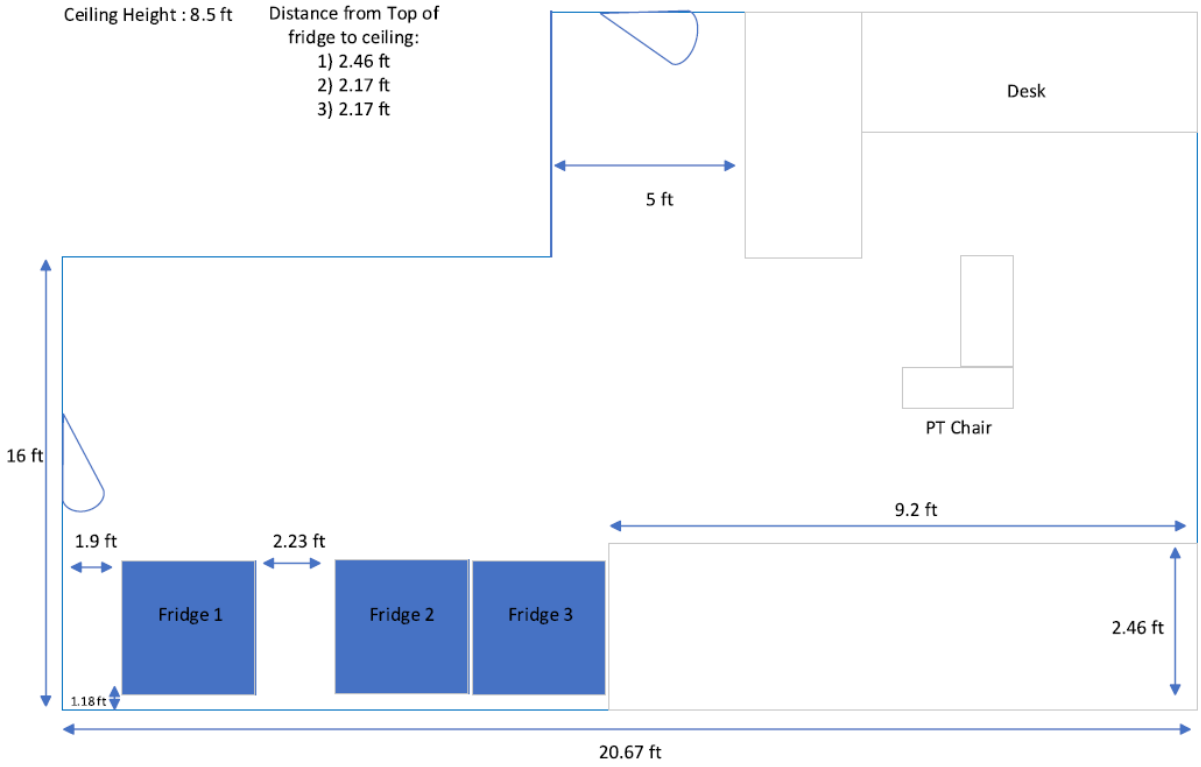
National Defence Headquarters
Ottawa, Ontario
K1A 0K2

Quartier général de la Défense nationale
Ottawa (Ontario)
K1A 0K2

Légende
Réfrigérateur / Refrigerator
Chaise du patient / Patient Chair
Bureau / Desk
pi / ft
Hauteur de plafond / Ceiling Height
Distance du haut du réfrigérateur au plafond / Distance from top of fridge to ceiling

Winnipeg

23 CFHSC - IMMUNZ RM 214 SCHEMATIC



ANNEXE « B » – BASE DE PAIEMENT

L'entrepreneur sera payé selon les prix unitaires fermes rendus au lieu de destination mentionné à l'annexe A.

L'entrepreneur est responsable du dédouanement à l'exportation, des frais de livraison, de l'administration, des coûts et des risques de transport. Le MDN est responsable de l'ensemble du dédouanement à l'importation, y compris le paiement des droits et taxes applicables. Le montant total de la taxe sur les produits et les services (TPS) ou de la taxe sur la vente harmonisée (TVH), s'il y a lieu, doit être indiqué séparément.

1.0 PÉRIODE INITIALE DU CONTRAT : DE LA DATE D'ATTRIBUTION DU CONTRAT AU 31 MARS 2024. TOUS LES ARTICLES DOIVENT ÊTRE LIVRÉS D'ICI LE 30 AOÛT 2023.

N^{O} DE L'ARTICLE	DESCRIPTION	Q^{TÉ}	UNITÉ DE DISTRIBUTION	PRIX UNITAIRE FERME ($ CA)
1.0	**ÉQUIPEMENT**			
1.1	Sonde émettrice pour les congélateurs à -80 °C, avec certificat d'étalonnage, conformément au paragraphe 2.1.1.1 de l'annexe A	Jusqu'à 5	Unitaire	**$[À insérer le montant au moment de l'attribution du contrat].**
1.2	Sonde émettrice pour les congélateurs à -20 °C, avec certificat d'étalonnage, conformément au paragraphe 2.1.1.1 de l'annexe A	Jusqu'à 30	Unitaire	**$[À insérer le montant au moment de l'attribution du contrat].**
1.3	Sonde émettrice pour les réfrigérateurs entre 2 °C et 8 °C, avec certificat d'étalonnage, conformément au paragraphe 2.1.1.1 de l'annexe A	Jusqu'à 61	Unitaire	**$[À insérer le montant au moment de l'attribution du contrat].**
1.4	Passerelle de réception dotée d'un routeur GSM, conformément au	1	Lot	**$[À insérer le montant au moment de l'attribution du**

	paragraphe 2.1.1.2 de l'annexe A			**contrat].**
1.5	Progiciel pour l'ensemble des sondes émettrices, sans limites du nombre d'utilisateurs et du nombre d'alarmes (téléphone, courriel ou message texte), conformément au paragraphe 2.1.2.1 de l'annexe A	1	Unitaire	**$[À insérer le montant au moment de l'attribution du contrat].**
1.6	Forfait cellulaire pour l'ensemble des passerelles de réception, conformément au paragraphe 2.1.2.2 de l'annexe A	1	Unitaire	**$[À insérer le montant au moment de l'attribution du contrat].**
2.0	**FORMATION**			
2.1	Séance d'instruction virtuelle des opérateurs pour 5 à 10 opérateurs, conformément au paragraphe 9.1 de l'annexe A	Jusqu'à 30	Séance	**$[À insérer le montant au moment de l'attribution du contrat].**
2.2	Séance d'instruction sur le soutien technique pour 2 à 8 technologues en génie biomédical, conformément au paragraphe 9.2 de l'annexe A	1	Séance	**$[À insérer le montant au moment de l'attribution du contrat].**

2.0 BESOINS OPTIONNELS : DU 1ER AVRIL 2024 AU 31 MARS 2027. TOUS LES ARTICLES DOIVENT ÊTRE LIVRÉS D'ICI LE 31 MARS 2027.

2.1 BESOINS OPTIONNELS – ANNÉE 1 : DU 1ER AVRIL 2024 AU 31 MARS 2025

N^{O} DE L'ARTICLE	DESCRIPTION	Q^{TE}	UNITÉ DE DISTRIBUTION	PRIX UNITAIRE FERME ($ CA)
1.0	**ÉQUIPEMENT**			

1.1	Tout type de sondes émettrices pour les congélateurs à -80 °C ou à -20 °C, ou les réfrigérateurs entre 2 °C à 8 °C, avec certificat d'étalonnage, conformément au paragraphe 2.2.1.1 de l'annexe A.	Jusqu'à 24	Unitaire	**$[À insérer le montant au moment de l'attribution du contrat].**
1.2	Passerelle de réception dotée d'un routeur GSM, conformément au paragraphe 2.2.1.2 de l'annexe A	Jusqu'à 6	Unitaire	**$[À insérer le montant au moment de l'attribution du contrat].**
1.3	Progiciel pour une (1) sonde émettrice supplémentaire, pour une période d'un (1) an, conformément au paragraphe 2.2.3.1 de l'annexe A	Jusqu'à 24	Unitaire	**$[À insérer le montant au moment de l'attribution du contrat].**
1.4	Forfait cellulaire pour une (1) passerelle de réception supplémentaire, pour une période d'un (1) an, conformément au paragraphe 2.2.3.3 de l'annexe A	Jusqu'à 6	Unitaire	**$[À insérer le montant au moment de l'attribution du contrat].**
1.5	Progiciel pour les sondes émettrices initiales, conformément au paragraphe 2.2.3.2 de l'annexe A	1	Unitaire	**$[À insérer le montant au moment de l'attribution du contrat].**
1.6	Forfait cellulaire pour les passerelles de réception initiales, conformément au paragraphe 2.2.3.4 de l'annexe A	1	Unitaire	**$[À insérer le montant au moment de l'attribution du contrat].**
1.7	Étalonnage hors site des sondes, conformément au paragraphe 2.2.2.3 de l'annexe A	1	Service	**$[À insérer le montant au moment de l'attribution du contrat].**
2.0	**FORMATION**			
2.1	Séance d'instruction virtuelle des opérateurs pour 5 à 10 opérateurs, conformément au	Jusqu'à 10	Séance	**$[À insérer le montant au moment de l'attribution du contrat].**

	paragraphe 9.1 de l'annexe A			
2.2	Séance d'instruction sur le soutien technique pour 2 à 8 technologues en génie biomédical, conformément au paragraphe 9.2 de l'annexe A	1	Séance	**$[À insérer le montant au moment de l'attribution du contrat].**

2.2 BESOINS OPTIONNELS – ANNÉE 2 : DU 1ER AVRIL 2025 AU 31 MARS 2026

N^{O} DE L'ARTICLE	DESCRIPTION	QTÉ	UNITÉ DE DISTRIBUTION	PRIX UNITAIRE FERME ($ CA)
1.0	**ÉQUIPEMENT**			
1.1	Tout type de sondes émettrices pour les congélateurs à -80 °C ou à -20 °C, ou les réfrigérateurs entre 2 °C à 8 °C, avec certificat d'étalonnage, conformément au paragraphe 2.2.1.1 de l'annexe A	Jusqu'à 24	Unitaire	**$[À insérer le montant au moment de l'attribution du contrat].**
1.2	Passerelle de réception dotée d'un routeur GSM, conformément au paragraphe 2.2.1.2 de l'annexe A	Jusqu'à 6	Unitaire	**$[À insérer le montant au moment de l'attribution du contrat].**
1.3	Progiciel pour une (1) sonde émettrice supplémentaire, pour une période d'un (1) an, conformément au paragraphe 2.2.3.1 de l'annexe A	Jusqu'à 48	Unitaire	**$[À insérer le montant au moment de l'attribution du contrat].**
1.4	Forfait cellulaire pour une (1) passerelle de réception supplémentaire, pour une période d'un (1) an, conformément au paragraphe 2.2.3.3 de l'annexe A	Jusqu'à 12	Unitaire	**$[À insérer le montant au moment de l'attribution du contrat].**
1.5	Progiciel pour les sondes émettrices initiales, conformément au paragraphe 2.2.3.2 de l'annexe A	1	Unitaire	**$[À insérer le montant au moment de l'attribution du contrat].**
1.6	Forfait cellulaire pour les passerelles de réception initiales, conformément au paragraphe 2.2.3.4 de l'annexe A	1	Unitaire	**$[À insérer le montant au moment de l'attribution du**

				contrat].
1.7	Étalonnage hors site des sondes, conformément au paragraphe 2.2.2.3 de l'annexe A	1	Service	**$[À insérer le montant au moment de l'attribution du contrat].**
2.0	**FORMATION**			
2.1	Séance d'instruction virtuelle des opérateurs pour 5 à 10 opérateurs, conformément au paragraphe 9.1 de l'annexe A	Jusqu'à 10	Séance	**$[À insérer le montant au moment de l'attribution du contrat].]**
2.2	Séance d'instruction sur le soutien technique pour 2 à 8 technologues en génie biomédical, conformément au paragraphe 9.2 de l'annexe A	1	Séance	**$[À insérer le montant au moment de l'attribution du contrat].**

2.3 BESOINS OPTIONNELS – ANNÉE 3 : DU 1ER AVRIL 2026 AU 31 MARS 2027

N^{O} DE L'ARTICLE	DESCRIPTION	Q^{TÉ}	UNITÉ DE DISTRIBUTION	PRIX UNITAIRE FERME ($ CA)
1.0	**ÉQUIPEMENT**			
1.1	Tout type de sondes émettrices pour les congélateurs à -80 °C ou à -20 °C, ou les réfrigérateurs entre 2 °C à 8 °C, avec certificat d'étalonnage, conformément au paragraphe 2.2.1.1 de l'annexe A	Jusqu'à 24	Unitaire	**$[À insérer le montant au moment de l'attribution du contrat].**
1.2	Passerelle de réception dotée d'un routeur GSM, conformément au paragraphe 2.2.1.2 de l'annexe A	Jusqu'à 6	Unitaire	**$[À insérer le montant au moment de l'attribution du contrat].**
1.3	Progiciel pour une (1) sonde émettrice supplémentaire, pour une période d'un (1) an, conformément au paragraphe 2.2.3.1 de l'annexe A	Jusqu'à 72	Unitaire	**$[À insérer le montant au moment de l'attribution du contrat].**
1.4	Forfait cellulaire pour une (1) passerelle de réception supplémentaire, pour une période d'un (1) an, conformément au paragraphe 2.2.3.3 de l'annexe A	Jusqu'à 18	Unitaire	**$[À insérer le montant au moment de l'attribution du contrat].**

1.5	Progiciel pour les sondes émettrices initiales, conformément au paragraphe 2.2.3.2 de l'annexe A	1	Unitaire	**$[À insérer le montant au moment de l'attribution du contrat].]**
1.6	Forfait cellulaire pour les passerelles de réception initiales, conformément au paragraphe 2.2.3.4 de l'annexe A	1	Unitaire	**$[À insérer le montant au moment de l'attribution du contrat].**
1.7	Étalonnage hors site des sondes, conformément au paragraphe 2.2.2.3 de l'annexe A	1	Service	**$[À insérer le montant au moment de l'attribution du contrat].**
2.0	**FORMATION**			
2.1	Séance d'instruction virtuelle des opérateurs pour 5 à 10 opérateurs, conformément au paragraphe 9.1 de l'annexe A	Jusqu'à 10	Séance	**$[À insérer le montant au moment de l'attribution du contrat].**
2.2	Séance d'instruction sur le soutien technique pour 2 à 8 technologues en génie biomédical, conformément au paragraphe 9.2 de l'annexe A	1	Séance	**$[À insérer le montant au moment de l'attribution du contrat].**

National Defence | Défense nationale

National Defence Headquarters
Ottawa, Ontario
K1A 0K2

Quartier général de la Défense nationale
Ottawa (Ontario)
K1A 0K2

ANNEXE « C » – LISTE DE VÉRIFICATION DES EXIGENCES RELATIVES À LA SÉCURITÉ

Government of Canada / Gouvernement du Canada

Contract Number / Numéro du contrat
W6369-22-A009 Amendment 1
Security Classification / Classification de sécurité
UNCLASSIFIED

SECURITY REQUIREMENTS CHECK LIST (SRCL)
LISTE DE VÉRIFICATION DES EXIGENCES RELATIVES À LA SÉCURITÉ (LVERS)

PART A - CONTRACT INFORMATION / PARTIE A - INFORMATION CONTRACTUELLE

1. Originating Government Department or Organization / Ministère ou organisme gouvernemental d'origine: **Department of National Defence**	2. Branch or Directorate / Direction générale ou Direction: DHSD/J4 Med Equip
3. a) Subcontract Number / Numéro du contrat de sous-traitance	3. b) Name and Address of Subcontractor / Nom et adresse du sous-traitant

4. Brief Description of Work / Brève description du travail

The Department of National Defence (DND) has a requirement for the supply of environmental monitoring systems fitted with data loggers and alarms to continuously and remotely monitor the temperature of 2 oC to 8 oC refrigerators as well as -20oC and -80oC freezers deployed for the storage of COVID-19 vaccines.

5. a) Will the supplier require access to Controlled Goods? Le fournisseur aura-t-il accès à des marchandises contrôlées?	☑ No / Non	☐ Yes / Oui
5. b) Will the supplier require access to unclassified military technical data subject to the provisions of the Technical Data Control Regulations? Le fournisseur aura-t-il accès à des données techniques militaires non classifiées qui sont assujetties aux dispositions du Règlement sur le contrôle des données techniques?	☑ No / Non	☐ Yes / Oui
6. Indicate the type of access required / Indiquer le type d'accès requis		
6. a) Will the supplier and its employees require access to PROTECTED and/or CLASSIFIED information or assets? Le fournisseur ainsi que les employés auront-ils accès à des renseignements ou à des biens PROTÉGÉS et/ou CLASSIFIÉS? (Specify the level of access using the chart in Question 7. c) (Préciser le niveau d'accès en utilisant le tableau qui se trouve à la question 7. c)	☐ No / Non	☑ Yes / Oui
6. b) Will the supplier and its employees (e.g. cleaners, maintenance personnel) require access to restricted access areas? No access to PROTECTED and/or CLASSIFIED information or assets is permitted. Le fournisseur et ses employés (p. ex. nettoyeurs, personnel d'entretien) auront-ils accès à des zones d'accès restreintes? L'accès à des renseignements ou à des biens PROTÉGÉS et/ou CLASSIFIÉS n'est pas autorisé.	☑ No / Non	☐ Yes / Oui
6. c) Is this a commercial courier or delivery requirement with **no** overnight storage? S'agit-il d'un contrat de messagerie ou de livraison commerciale **sans** entreposage de nuit?	☑ No / Non	☐ Yes / Oui

7. a) Indicate the type of information that the supplier will be required to access / Indiquer le type d'information auquel le fournisseur devra avoir accès

Canada ☑	NATO / OTAN ☐	Foreign / Étranger ☐
7. b) Release restrictions / Restrictions relatives à la diffusion		
No release restrictions / Aucune restriction relative à la diffusion ☑	All NATO countries / Tous les pays de l'OTAN ☐	No release restrictions / Aucune restriction relative à la diffusion ☐
Not releasable / À ne pas diffuser ☐		
Restricted to: / Limité à : ☐	Restricted to: / Limité à : ☐	Restricted to: / Limité à : ☐
Specify country(ies): / Préciser le(s) pays :	Specify country(ies): / Préciser le(s) pays :	Specify country(ies): / Préciser le(s) pays :
7. c) Level of information / Niveau d'information		
PROTECTED A / PROTÉGÉ A ☑	NATO UNCLASSIFIED / NATO NON CLASSIFIÉ ☐	PROTECTED A / PROTÉGÉ A ☐
PROTECTED B / PROTÉGÉ B ☐	NATO RESTRICTED / NATO DIFFUSION RESTREINTE ☐	PROTECTED B / PROTÉGÉ B ☐
PROTECTED C / PROTÉGÉ C ☐	NATO CONFIDENTIAL / NATO CONFIDENTIEL ☐	PROTECTED C / PROTÉGÉ C ☐
CONFIDENTIAL / CONFIDENTIEL ☐	NATO SECRET / NATO SECRET ☐	CONFIDENTIAL / CONFIDENTIEL ☐
SECRET / SECRET ☐	COSMIC TOP SECRET / COSMIC TRÈS SECRET ☐	SECRET / SECRET ☐
TOP SECRET / TRÈS SECRET ☐		TOP SECRET / TRÈS SECRET ☐
TOP SECRET (SIGINT) / TRÈS SECRET (SIGINT) ☐		TOP SECRET (SIGINT) / TRÈS SECRET (SIGINT) ☐

If Yes, classify this form by annotating the top and bottom in the area entitled "Security Classification" and indicate with attachments (e.g. SECRET with Attachments).
Dans l'affirmative, classifier le présent formulaire en indiquant le niveau de sécurité dans la case intitulée « Classification de sécurité » au haut et au bas du formulaire et indiquer qu'il y a des pièces jointes (p. ex. SECRET avec des pièces jointes).

National Defence | Défense nationale

National Defence Headquarters
Ottawa, Ontario
K1A 0K2

Quartier général de la Défense nationale
Ottawa (Ontario)
K1A 0K2

Government of Canada | Gouvernement du Canada

Contract Number / Numéro du contrat
W6369-22-A009 Amendment 1
Security Classification / Classification de sécurité UNCLASSIFIED

PART A *(continued)* / PARTIE A *(suite)*

8. Will the supplier require access to PROTECTED and/or CLASSIFIED COMSEC information or assets? — ☑ No / Non ☐ Yes / Oui
Le fournisseur aura-t-il accès à des renseignements ou à des biens COMSEC désignés PROTÉGÉS et/ou CLASSIFIÉS?
If Yes, indicate the level of sensitivity:
Dans l'affirmative, indiquer le niveau de sensibilité :

9. Will the supplier require access to extremely sensitive INFOSEC information or assets? — ☑ No / Non ☐ Yes / Oui
Le fournisseur aura-t-il accès à des renseignements ou à des biens INFOSEC de nature extrêmement délicate?

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

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

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

☑ RELIABILITY STATUS / COTE DE FIABILITÉ	☐ CONFIDENTIAL / CONFIDENTIEL	☑ SECRET / SECRET	☐ TOP SECRET / TRÈS SECRET
☐ TOP SECRET– SIGINT / TRÈS SECRET – SIGINT	☐ NATO CONFIDENTIAL / NATO CONFIDENTIEL	☐ NATO SECRET / NATO SECRET	☐ COSMIC TOP SECRET / COSMIC TRÈS SECRET
☐ SITE ACCESS / ACCÈS AUX EMPLACEMENTS			

Special comments:
Commentaires spéciaux : Secret required only for those identified in the Cloud IT Security Obligations document, serial 29 para c.

NOTE: If multiple levels of screening are identified, a Security Classification Guide must be provided.
REMARQUE : Si plusieurs niveaux de contrôle de sécurité sont requis, un guide de classification de la sécurité doit être fourni.

10. b) May unscreened personnel be used for portions of the work? — ☑ No / Non ☐ Yes / Oui
Du personnel sans autorisation sécuritaire peut-il se voir confier des parties du travail?
If Yes, will unscreened personnel be escorted? — ☑ No / Non ☐ Yes / Oui
Dans l'affirmative, le personnel en question sera-t-il escorté?

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

INFORMATION / ASSETS / RENSEIGNEMENTS / BIENS

11. a) Will the supplier be required to receive and store PROTECTED and/or CLASSIFIED information or assets on its site or premises? — ☐ No / Non ☑ Yes / Oui
Le fournisseur sera-t-il tenu de recevoir et d'entreposer sur place des renseignements ou des biens PROTÉGÉS et/ou CLASSIFIÉS?

11. b) Will the supplier be required to safeguard COMSEC information or assets? — ☑ No / Non ☐ Yes / Oui
Le fournisseur sera-t-il tenu de protéger des renseignements ou des biens COMSEC?

PRODUCTION

11. c) Will the production (manufacture, and/or repair and/or modification) of PROTECTED and/or CLASSIFIED material or equipment occur at the supplier's site or premises? — ☑ No / Non ☐ Yes / Oui
Les installations du fournisseur serviront-elles à la production (fabrication et/ou réparation et/ou modification) de matériel PROTÉGÉ et/ou CLASSIFIÉ?

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

11. d) Will the supplier be required to use its IT systems to electronically process, produce or store PROTECTED and/or CLASSIFIED information or data? — ☐ No / Non ☑ Yes / Oui
Le fournisseur sera-t-il tenu d'utiliser ses propres systèmes informatiques pour traiter, produire ou stocker électroniquement des renseignements ou des données PROTÉGÉS et/ou CLASSIFIÉS?

11. e) Will there be an electronic link between the supplier's IT systems and the government department or agency? — ☑ No / Non ☐ Yes / Oui
Disposera-t-on d'un lien électronique entre le système informatique du fournisseur et celui du ministère ou de l'agence gouvernementale?

National Defence | Défense nationale

National Defence Headquarters
Ottawa, Ontario
K1A 0K2

Quartier général de la Défense nationale
Ottawa (Ontario)
K1A 0K2

Government of Canada | Gouvernement du Canada

Contract Number / Numéro du contrat
W6369-22-A009 Amendment 1
Security Classification / Classification de sécurité
UNCLASSIFIED

PART C - *(continued)* / PARTIE C - *(suite)*

For users completing the form **manually** use the summary chart below to indicate the category(ies) and level(s) of safeguarding required at the supplier's site(s) or premises.
Les utilisateurs qui remplissent le formulaire **manuellement** doivent utiliser le tableau récapitulatif ci-dessous pour indiquer, pour chaque catégorie, les niveaux de sauvegarde requis aux installations du fournisseur.

For users completing the form **online** (via the Internet), the summary chart is automatically populated by your responses to previous questions.
Dans le cas des utilisateurs qui remplissent le formulaire **en ligne** (par Internet), les réponses aux questions précédentes sont automatiquement saisies dans le tableau récapitulatif.

SUMMARY CHART / TABLEAU RÉCAPITULATIF

Category / Catégorie	PROTECTED / PROTÉGÉ			CLASSIFIED / CLASSIFIÉ			NATO				COMSEC					
	A	B	C	CONFIDENTIAL / CONFIDENTIEL	SECRET	TOP SECRET / TRÈS SECRET	NATO RESTRICTED / NATO DIFFUSION RESTREINTE	NATO CONFIDENTIAL / NATO CONFIDENTIEL	NATO SECRET	COSMIC TOP SECRET / COSMIC TRÈS SECRET	PROTECTED / PROTÉGÉ A	PROTECTED / PROTÉGÉ B	PROTECTED / PROTÉGÉ C	CONFIDENTIAL / CONFIDENTIEL	SECRET	TOP SECRET / TRES SECRET
Information / Assets / Renseignements / Biens	✓															
Production																
IT Media / Support TI	✓															
IT Link / Lien électronique																

12. a) Is the description of the work contained within this SRCL PROTECTED and/or CLASSIFIED?
La description du travail visé par la présente LVERS est-elle de nature PROTÉGÉE et/ou CLASSIFIÉE?

☑ No / Non ☐ Yes / Oui

If Yes, classify this form by annotating the top and bottom in the area entitled "Security Classification".
Dans l'affirmative, classifier le présent formulaire en indiquant le niveau de sécurité dans la case intitulée « Classification de sécurité » au haut et au bas du formulaire.

12. b) Will the documentation attached to this SRCL be PROTECTED and/or CLASSIFIED?
La documentation associée à la présente LVERS sera-t-elle PROTÉGÉE et/ou CLASSIFIÉE?

☑ No / Non ☐ Yes / Oui

If Yes, classify this form by annotating the top and bottom in the area entitled "Security Classification" and indicate with attachments (e.g. SECRET with Attachments).
Dans l'affirmative, classifier le présent formulaire en indiquant le niveau de sécurité dans la case intitulée « Classification de sécurité » au haut et au bas du formulaire et indiquer qu'il y a des pièces jointes (p. ex. SECRET avec des pièces jointes).

National Defence | Défense nationale

National Defence Headquarters
Ottawa, Ontario
K1A 0K2

Quartier général de la Défense nationale
Ottawa (Ontario)
K1A 0K2

[Page 4 de la LVERS à insérer dans le contrat subséquent]

National Defence | Défense nationale

National Defence Headquarters
Ottawa, Ontario
K1A 0K2

Quartier général de la Défense nationale
Ottawa (Ontario)
K1A 0K2

APPENDICE 1 DE L'ANNEXE «C»- (LVERS) GUIDE DE SÉCURITÉ SUPPLÉMENTAIRE

Partie A - Restrictions multiples relative à la Diffusion : GUIDE DE SÉCURITÉ

À remplir en supplément à la case 7b) lorsque des Restrictions relatives à la diffusion sont identifiées. Veuillez indiquer à quel niveau d'information que les restrictions relatives à la diffusion s'appliquent. Veuillez indiquer dans le tableau si un niveau d'information comprend des restrictions multiples, *c'est-à-dire* si une portion des renseignements SECRET porte la mise en garde RÉSERVÉ AUX CANADIENS et les autres portions SECRET n'ont aucune restriction relative à la diffusion.

Renseignements canadiens

Restriction due à la citoyenneté	PROTÉGÉ			CLASSIFIÉ			
	A	B	C	CONFIDENTIEL	SECRET	TRÈS SECRET	TRÈS SECRET (SIGINT)
Aucune restriction relative à la diffusion	x						
À ne pas diffuser							
Limité à :							
Résidents permanents inclus *							

Renseignements OTAN

Restriction due à la citoyenneté	NATO NON CLASSIFIÉ	NATO DIFFUSION RESTREINTE	NATO CONFIDENTIEL	NATO SECRET	COSMIC TRÈS SECRET
Tous les pays de l'OTAN					
Limité à:					
Résidents permanents inclus *					

Renseignements étrangers

Restriction due à la citoyenneté	PROTÉGÉ			CLASSIFIÉ			
	A	B	C	CONFIDENTIEL	SECRET	TRÈS SECRET	TRÈS SECRET (SIGINT)
Aucune restriction relative à la diffusion							
Limité à:							
Résidents permanents inclus *							

Renseignements COMSEC

Restriction due à la citoyenneté	PROTÉGÉ			CLASSIFIÉ			
	A	B	C	CONFIDENTIEL	SECRET	TRÈS SECRET	TRÈS SECRET (SIGINT)
À ne pas diffuser							
Limité à:							

*** Lorsqu'une restriction relative à la diffusion est indiquée, veuillez spécifier si les résidents permanents seront inclus.**

National Defence | Défense nationale

National Defence Headquarters
Ottawa, Ontario
K1A 0K2

Quartier général de la Défense nationale
Ottawa (Ontario)
K1A 0K2

Partie B – Multiples niveaux de Contrôle de la sécurité du personnel: GUIDE DE CLASSIFICATION DE LA SÉCURITÉ **À remplir en supplément à la case 10a) lorsque de multiples niveaux de Contrôle de la sécurité du personnel sont identifiés. Veuillez indiquer quels niveaux de sécurité du personnel seront requis pour quelles portions du travail et/ou accès dans le contrat.**			
Niveau de Sécurité du personnel (i.e. Fiabilité, Secret)	Poste / Description / Tâche	Accès à des sites et/ou des renseignements. Niveau d'information auquel on aura accès.	Restriction due à la citoyenneté (s'il y en a)
Fiabilité	Personnel contractuel ayant accès aux données du MDN	Des privilèges système selon le critère du moindre privilège; cela signifie qu'il faut appliquer l'ensemble plus restrictif de privilèges et le principe du besoin de savoir (c.-à-d. limiter l'accès aux renseignements aux personnes qui en ont besoin dans le cadre de leurs fonctions) nécessaires à l'exécution des tâches autorisées.	
Secret	Administrateur de système en nuage ou utilisateurs privilégiés	La gestion et la maintenance du SI du nuage du contrat doivent être assurées par une ou plusieurs personnes qui possèdent, à tout le moins, une cote de sécurité de niveau Secret (niveau II) valide.	

Partie C – Mesures de protection / Technologie de l'Information (TI) – 11d = oui
Les besoins de sécurité TI doivent être spécifiés dans un document technique distinct et soumis avec la LVERS.

AUTRES DIRECTIVES DE SÉCURITÉ

Le personnel contractuel doit posséder une cote de fiabilité, sauf indication contraire dans le document « Obligations de sécurité relatives aux TI infonuagiques »

National Defence | Défense nationale

National Defence Headquarters
Ottawa, Ontario
K1A 0K2

Quartier général de la Défense nationale
Ottawa (Ontario)
K1A 0K2

APPENDICE 2 DE L'ANNEXE «C» – EXIGENCES EN MATIÈRE DE SÉCURITÉ DES TI

Ministère de la Défense nationale (MDN)

Document sur les exigences relatives à la sécurité des TI

pour le

Contrat W6369-22-A009 Modification 1

1. Introduction

1.1 Document sur les exigences en matière de sécurité des technologies de l'information (TI). Le présent document, intitulé « Document sur les exigences relatives à la sécurité des TI pour le contrat W6369-22-A009 Modification 1 » est fourni conformément aux instructions pour remplir la partie C, section 11. d), du formulaire 350-103 du Secrétariat du Conseil du Trésor (SCT) :

> « Le fournisseur sera-t-il tenu d'utiliser ses propres systèmes informatiques pour traiter, produire ou stocker électroniquement des renseignements ou des données PROTÉGÉS et CLASSIFIÉS? Si la réponse est oui, le ministère ou l'organisme client devra préciser les exigences en matière de sécurité des TI relativement à cet achat dans un document technique distinct… »

Chacun des documents sur les exigences relatives à la sécurité des TI ne s'applique qu'au contrat pour lequel il a été rédigé. Par conséquent le présent document, intitulé « Document sur les exigences relatives à la sécurité des TI pour le contrat W6369-22-A009 Modification 1 » est spécifique au contrat W6369-22-A009 Modification 1.

1.2 Exigences en matière de sécurité des TI du MDN. Le présent document décrit les exigences en matière de sécurité des TI du MDN quant au stockage, au traitement et à la création électroniques de renseignements de nature exclusive de niveau Protégé A et moins du présent contrat.

1.3 Renseignements exclusifs. Dans le présent document uniquement, l'expression « renseignements exclusifs » désigne tous les biens et renseignements de nature délicate (désignés ou classifiés) du gouvernement que stocke, traite et produit un organisme privé quelconque pour exécuter un contrat conclu avec le MDN, contrat dont la sécurité est assurée par l'intermédiaire du Programme de sécurité des contrats de Services publics et Approvisionnement Canada (PSC de SPAC).

1.4 Critères de connectivité d'un lien électronique. Dans l'éventualité où le système d'information (SI) utilisé pour stocker, traiter et créer les renseignements de nature exclusive devrait également se connecter électroniquement à l'infrastructure du MDN (c.-à-d. que la case « Oui » a été cochée à la partie C, section 11.e de la Liste de vérification des exigences relatives à la sécurité [LVERS]), l'officier de projet préparera, à l'intention du Bureau de gestion de projet (BGP) du MDN, un document « Critères de connectivité » distinct pour le lien électronique, et ce lien devra être validé et autorisé par le PSC de SPAC.

1.5 Couches de protection de la sécurité. La sécurité repose sur diverses couches de protection. En d'autres termes, les exigences relatives à la sécurité des TI, lorsqu'elles sont respectées, permettent de protéger l'information efficacement seulement si d'autres mesures et politiques de sécurité les sous-tendent. On ne doit réaliser des travaux confiés à contrat qu'après avoir mis en œuvre des mesures de sécurité matérielle, du personnel, des procédures, des renseignements et des TI.

1.6 Autres renseignements. Le Manuel de la sécurité des contrats (MSC), que l'on peut se procurer auprès de SPAC, définit les procédures que les organisations canadiennes doivent appliquer pour protéger l'information et les biens du gouvernement. Des renseignements supplémentaires sur la sécurité sont offerts sur Internet par le PSC de SPAC, de même que le Centre de la sécurité des télécommunications (CST), le Centre canadien pour la cybersécurité (CCC) et la Gendarmerie royale du Canada (GRC).

2. Exigences préalables obligatoires

2.1 Validation de SPAC

2.1.1 Manuel de la sécurité des contrats (MSC). En plus des exigences relatives à la sécurité énoncées dans le MSC, les autres exigences décrites dans le présent document doivent être respectées. Lorsque deux exigences traitent du même enjeu, celle la plus contraignante doit être appliquée.

2.1.2 Sites de l'entrepreneur. L'entrepreneur doit préciser au PSC de SPAC et à l'officier de projet du MDN tous les sites physiques utilisés pour stocker, traiter et créer les renseignements de nature exclusive de niveau Protégé A du présent contrat. Cela comprend tout bureau principal ou de rechange applicable de l'entrepreneur, tout chantier de construction, tout emplacement de stockage des sauvegardes, tout partenaire, tout bureau de sous-traitants à tous les niveaux, etc.

2.1.3 Exigences du site. Chaque site utilisé pour stocker, traiter et créer électroniquement les renseignements de nature exclusive du présent contrat doit se voir attribuer une habilitation de sécurité d'installation ainsi qu'une vérification des organismes désignés (VOD) ou une autorisation de détenir des renseignements (ADR), s'il y a lieu. Chaque site doit aussi avoir reçu une habilitation de sécurité du PSC de SPAC avant d'être autorisé à stocker, à traiter et à créer électroniquement des renseignements de nature exclusive.

2.2 Sécurité physique

2.2.1 Autorisation des installations. Les activités de stockage, de traitement et de création des renseignements de nature exclusive du présent contrat ne peuvent être menées que dans des installations autorisées par le PSC de SPAC. Toutes les données doivent être stockées, traitées et créées de manière sécuritaire, de façon à en prévenir la visualisation, l'accès et la manipulation non autorisés.

2.2.2 Zones de sécurité matérielle. Conformément au *Guide pour l'établissement des zones de sécurité matérielle G1-026* de la GRC, le SI doit être installé et exploité dans une zone de travail ou une zone de travail temporaire.

2.2.3 Renseignements de nature exclusive à l'extérieur du Canada. Les activités de stockage, de traitement et de création de renseignements de nature exclusive à l'extérieur du Canada ne sont pas autorisées dans le cadre du présent contrat.

2.2.4 Télétravail et informatique mobile. Dans le cadre du présent contrat, il n'est pas permis d'effectuer des tâches liées au SI ou aux renseignements exclusifs en télétravail ou au moyen de l'informatique mobile.

2.3 Sécurité du personnel

2.3.1 Habilitation de sécurité du personnel. Tous les membres du personnel de l'entrepreneur qui ont accès à des renseignements exclusifs doivent :

2.3.1.1 détenir, à tout le moins, une habilitation de sécurité valide décernée par le PSC de SPAC, laquelle doit faire l'objet d'un suivi;

2.3.1.2 se voir attribuer les privilèges système selon le critère du moindre privilège. Cela signifie qu'il faut appliquer l'ensemble le plus restrictif de privilèges et le principe du

besoin de savoir (à savoir, limiter l'accès à l'information uniquement à ceux qui en ont besoin dans le cadre de leurs fonctions) nécessaires à l'exécution des tâches autorisées;

2.3.1.3 être citoyen canadien.

2.3.2 Accès à la zone de sécurité matérielle. Aucun visiteur, étranger ou membre du personnel non autorisé ne doit avoir accès aux renseignements exclusifs, au SI ou à la zone où l'on traite, produit ou stocke les renseignements exclusifs, à moins de détenir une cote de fiabilité valide et d'être accompagné par un employé autorisé de l'entrepreneur. Un journal de vérification doit être tenu à jour au sujet de tout visiteur, de tout ressortissant étranger ou de tout membre non autorisé du personnel accédant à la zone de travail.

2.3.3 Formation sur la sensibilisation à la sécurité des TI. Tout le personnel de l'entrepreneur traitant des renseignements de nature exclusive doit assister aux séances de formation et d'information coordonnées et animées par l'agent de sécurité d'entreprise (ASE) ou l'agent remplaçant de sécurité d'entreprise (ARSE). La formation doit, à tout le moins, renvoyer au MSC de SPAC et à tout autre renseignement sur la sécurité dont l'officier de projet du MDN décidera de la pertinence, ainsi qu'aux ordonnances de sécurité et aux instructions permanentes d'opérations (IPO) relatives au système pour le SI. La formation doit également traiter de l'ingénierie sociale, de l'utilisation des médias sociaux et de la connaissance de la situation.

2.4 Sécurité des procédures

2.4.1 Ordonnances de sécurité des TI et instructions permanentes d'opérations. L'entrepreneur doit rédiger des ordres de sécurité et des IPO ayant spécifiquement trait au SI, à son exploitation et à sa maintenance pour le SI. Ces documents doivent, à tout le moins, traiter des éléments suivants :

2.4.1.1 les rôles et responsabilités (p. ex., de l'ASE, du responsable technique ou de l'administrateur système pour le SI);

2.4.1.2 la gestion de l'accès pour la zone de travail et le SI;

2.4.1.3 l'utilisation acceptable du SI;

2.4.1.4 les procédures de gestion des incidents;

2.4.1.5 tout autre sujet précisé dans le présent document;

2.4.1.6 tout autre enjeu ou problème relevé par l'officier de projet du MDN ou le BGP durant la période de validité du présent contrat.

2.4.2 Formulaire de consentement de l'utilisateur. Chaque membre du personnel qui a accès au SI doit prendre connaissance des ordonnances de sécurité des TI qui s'y rapportent pour le SI, ainsi que lire et signer le formulaire de consentement de l'utilisateur, tel que rédigé et suivi par l'ASE ou l'ARSE. Toutes les modifications apportées aux ordonnances de sécurité des TI propres au système, aux IPO ou au formulaire de consentement de l'utilisateur doivent être communiquées à tout le personnel ayant accès au SI.

2.4.3 Administrateur système – Habilitation de sécurité du personnel. Le SI doit être administré et maintenu à l'interne par une ou des personnes détenant, à tout le moins, une habilitation de sécurité valide et une **cote de sécurité de niveau « secret » (niveau II)** pour les utilisateurs privilégiés et les administrateurs de système du SI infonuagique du contrat.

2.4.4 Gestion des vulnérabilités et signalement des incidents. Selon l'annexe A, section VI du MSC, l'entrepreneur doit établir et appliquer une procédure de gestion des vulnérabilités pour gérer les risques liés aux vulnérabilités. Il doit également signaler tout incident de sécurité à l'officier de projet du MDN au plus tard 24 heures après sa détection ou son signalement à SPAC.

2.4.5 Surveillance continue du SI. L'entrepreneur doit assurer une surveillance continue de sa posture de sécurité, y compris la sécurité matérielle, du personnel, des procédures, des renseignements et des TI. Il doit faire part au PSC de SPAC et à l'officier de projet du MDN de tout enjeu qui pourrait avoir une incidence sur la sécurité des renseignements de nature exclusive ou du SI.

2.5 Sécurité de l'information

2.5.1 Marquage des documents. Qu'ils soient sur support papier ou en version électronique, tous les documents renfermant des renseignements de nature exclusive doivent être marqués d'après le niveau de sensibilité le plus élevé des renseignements qu'ils contiennent et se voir attribuer un identificateur exclusif afin d'assurer un contrôle et un suivi adéquats.

2.5.2 Protection des renseignements statiques. L'entrepreneur doit protéger la sécurité des renseignements de nature exclusive statiques au moyen de mesures de sécurité matérielle et de TI.

2.5.2.1 Lorsqu'ils sont laissés sans surveillance, tous les documents imprimés qui contiennent des renseignements exclusifs et tous les supports informatiques amovibles utilisés pour conserver, traiter ou produire ce type d'information doivent être rangés dans des contenants sécurisés et verrouillés du gouvernement du Canada. Le choix du contenant dépend du niveau de confidentialité de l'information ainsi stockée. Les coffres doivent être conformes au document *G1-001 – Guide d'équipement de sécurité* de la GRC; ce document n'étant pas accessible au grand public, l'entrepreneur peut communiquer avec l'officier de projet du MDN pour obtenir des renseignements à ce sujet.

2.5.2.2 Laissé sans surveillance, le contenu de tous les supports informatiques amovibles utilisés pour conserver, traiter ou produire des renseignements exclusifs doit être chiffré avec une technologie approuvée par le GC et correspondant au niveau de confidentialité de l'information ainsi stockée. De cette façon, les renseignements exclusifs sont protégés si le support est perdu, égaré ou volé.

2.5.2.3 Seuls les membres du personnel de l'entrepreneur autorisés à accéder aux renseignements exclusifs disposeront des outils nécessaires pour déchiffrer le contenu des documents électroniques et auront accès aux différentes clés et combinaisons des contenants sécurisés approuvés.

2.5.3 Échange de renseignements de nature exclusive. Lorsque le MDN et tous les niveaux d'entrepreneurs et de sous-traitants s'échangent des renseignements de nature exclusive sur support papier et support de TI amovible, tous les documents sur support papier et tous les supports de TI amovibles doivent être manipulés et transportés ou transmis conformément aux lignes directrices du GC énoncées dans le MSC ou au document *G1-009 – Transport et transmission de renseignements protégés ou classifiés* de la GRC. Lorsqu'ils sont transportés (c.-à-d. déplacés à la main d'une personne ou d'un lieu à une autre personne ou à un autre lieu par une personne ayant un besoin de savoir et détenant l'habilitation de sécurité correspondant au niveau le plus élevé des renseignements de nature exclusive) ou transmis (c.-à-d. envoyés d'une personne ou d'un lieu à une autre personne ou à un autre lieu par un tiers), tous les

supports électroniques doivent être chiffrés au moyen de la technologie de chiffrement approuvée par le GC selon le niveau de sensibilité le plus élevé des renseignements qu'ils contiennent.

2.5.4 Échange de renseignements de nature exclusive – Emballage. Tous les documents sur support papier et tous les supports de TI doivent être emballés de la manière appropriée; une lettre de présentation et un formulaire de transmission ou un bordereau de circulation doivent les accompagner et fournir les renseignements suivants :

2.5.4.1 le niveau de sensibilité le plus élevé des renseignements contenus dans l'emballage;

2.5.4.2 la date du transport ou de la transmission;

2.5.4.3 l'identificateur exclusif de chaque document ou chaque support de TI contenu dans l'emballage;

2.5.4.4 le nom en caractères d'imprimerie et le numéro de téléphone de l'expéditeur;

2.5.4.5 la signature de l'expéditeur;

2.5.4.6 l'adresse postale de la destination;

2.5.4.7 le nom en caractères d'imprimerie et le numéro de téléphone du destinataire;

2.5.4.8 la signature du destinataire.

2.5.5 Autorisation de liens électroniques. L'échange de renseignements de nature exclusive avec les partenaires, les sous-traitants ou le MDN ne doit pas s'effectuer au moyen de liens électroniques. Tout lien technologique doit d'abord être validé, inspecté et autorisé par le PSC de SPAC ainsi que reconnu et autorisé par l'autorité de la sécurité des TI du MDN et l'officier de projet du MDN.

2.5.6 Séparation des renseignements de nature exclusive en vue d'une destruction d'urgence. Il faut séparer tous les renseignements de nature exclusive (p. ex., les documents sur support papier et les supports de TI) des autres renseignements contractuels et ministériels afin de pouvoir les détruire ou les effacer de manière sûre, immédiatement à la demande du PSC de SPAC ou de l'officier de projet du MDN, de la manière indiquée dans la publication *Nettoyage des supports de TI (ITSP.40.006)* du CST.

Marchandises contrôlées. Dans le cadre du présent contrat, l'entrepreneur n'aura pas besoin d'accéder à des biens ou à des renseignements relatifs à des marchandises contrôlées.

2.5.7 Sous-traitants. L'entrepreneur doit préciser à l'officier de projet du MDN tous les partenaires de même que tous les niveaux de partenariat et de sous-traitants qui participent à la réalisation du contrat et enregistrer officiellement ces entités auprès du PSC de SPAC. En définitive, il incombe à l'entrepreneur de veiller à ce que toutes les exigences relatives à la sécurité et tous les documents de sécurité pertinents ou connexes relatifs au présent contrat soient fournis aux partenaires de l'entrepreneur et à tous les niveaux de sous-traitants.

2.5.8 Exigences en matière de sécurité des TI des contrats de sous-traitance. Toutes les exigences pertinentes en matière de sécurité des TI doivent également être comprises dans les contrats de sous-traitance.

3. Exigences minimales en matière de sécurité des TI

3.1 Vérification de la conformité aux politiques en matière de sécurité des TI

Le MDN se réserve le droit d'inspecter, selon une fréquence et un calendrier que déterminera le responsable de la sécurité des TI du MDN, chaque installation de l'entrepreneur servant au présent contrat, afin d'assurer la conformité aux exigences en matière de sécurité des TI énoncées dans le présent document ainsi qu'aux exigences et politiques du GC en matière de prévention, de détection, d'intervention et de reprise.

3.2 Configuration du système technologique

3.2.1 Configuration du système de base. L'officier de projet du MDN prévoit que la configuration du système de base sera un réseau de sondes émettrices commerciales avec une capacité sans fil à courte portée et de passerelles de réception dotées d'un routeur GSM fournies par l'entrepreneur. Les utilisateurs des FAC auront leur appareil personnel (portables, tablettes, téléphones cellulaires).

3.2.2 Type de système. Le SI peut être configuré comme segment de réseau, c'est-à-dire la partie de l'infrastructure de réseau d'un entrepreneur qui a été autorisée à traiter, à produire et à stocker les renseignements exclusifs. Des mécanismes de sécurité additionnels seront nécessaires pour séparer les renseignements exclusifs des autres données de l'entrepreneur. Il comprend également une capacité de GSM.

3.2.3 Sécurité du réseau. Si le SI est configuré comme un réseau, l'entrepreneur doit mettre en place des mesures de défense du périmètre et de sécurité du réseau (p. ex., des pare-feu) afin de gérer le trafic et de protéger les serveurs et l'équipement de TI accessibles de l'extérieur.

3.2.4 Séparation du SI. Si le SI est configuré comme un segment du réseau de l'entrepreneur, ce dernier doit séparer son réseau en zones de sécurité de TI et mettre en place des mesures de défense du périmètre et de sécurité du réseau. Le CST et le CCC fournissent des lignes directrices à ce sujet : « Établissement des zones de sécurité dans un réseau – Considérations de conception relatives au positionnement des services dans les zones (ITSG-38) » et « Exigences de base en matière de sécurité pour les zones de sécurité de réseau au sein du gouvernement du Canada (ITSG-22) ». Les détails de la méthodologie de séparation (c.-à-d. le diagramme topologique et autres documents jugés nécessaires) doivent être fournis au PSC de SPAC et à l'officier de projet du MDN aux fins d'évaluation.

3.2.5 Type d'équipement. L'équipement servant à stocker, à traiter et à produire des renseignements exclusifs peut être composé de produits commerciaux sur étagère.

3.2.6 Disques durs du SI. L'équipement de traitement peut être configuré avec des disques durs internes. Les postes de travail (PC, portables ou tablettes), les serveurs, les périphériques de stockage de TI (stockage en réseau [NAS] et zone de stockage en réseaux [SAN]), les imprimantes et les scanneurs constituent des exemples d'équipement de traitement pour ce SI.

3.2.7 Systèmes d'exploitation. Tout l'équipement de TI utilisé dans le cadre du SI doit être doté d'un système d'exploitation compatible, c'est-à-dire que le fournisseur du système d'exploitation doit créer les correctifs de sécurité nécessaires et fournir sa version la plus récente. Il faut installer ceux-ci régulièrement, au moins une fois par mois. Le système d'exploitation doit être renforcé, c'est-à-dire qu'il doit être configuré pour désactiver les processus, services et ports inutiles. Les IPO relatives au SI doivent indiquer la configuration du système d'exploitation, la

fréquence à laquelle les correctifs de sécurité sont appliqués au système d'exploitation, ainsi que la méthode utilisée pour ce faire.

3.2.8 Logiciels antivirus et antimaliciels. Tout l'équipement de TI applicable doit être doté d'un logiciel antivirus/antimaliciels. Il faut mettre à jour régulièrement les fichiers de définition connexes, au moins deux fois par semaine ou préférablement chaque jour. Les IPO relatives au SI doivent indiquer la fréquence et la méthode employée pour effectuer cette mise à jour ainsi que la configuration de l'application antivirus. Cette configuration doit :

3.2.8.1 permettre les modifications apportées seulement par les administrateurs système;

3.2.8.2 analyser automatiquement l'équipement de TI applicable du SI à sa mise sous tension ou à des intervalles de temps préétablis, soit au moins une fois par semaine;

3.2.8.3 analyser chaque nouveau fichier ajouté au SI afin d'y déceler tout code malveillant éventuel.

3.2.9 Logiciels et applications. Seules les applications nécessaires en vertu du présent contrat doivent être installées sur le SI. Les correctifs des applications doivent être tenus à jour et gérés selon un processus défini de gestion de la configuration. Les IPO relatives au SI doivent préciser chaque application installée et sa version, de même que le processus de gestion des correctifs des applications. Voici les exigences et les recommandations minimales en matière de sécurité des TI pour la solution de sécurité de la plateforme Web (logiciel) utilisée pour surveiller les réfrigérateurs et les congélateurs.

3.2.9.1 La plateforme Web doit utiliser un protocole de transfert hypertexte sécurisé (HTTPS) pour assurer des communications sécurisées (chiffrés) avec le plus récent protocole de sécurité de la couche transport (TLS), comme TLS 1.2 ou 1.3. Pour sécuriser les services Web, respecter les lignes directrices énoncées dans le NIST SP 800-95 et les lignes directrices en matière de chiffrement des services Web et respecter les lignes directrices énoncées dans le NIST SP 800-175A, SP-800-175B Rev.1 et les modules FIPS 140-2 et FIPS 186-4.

3.2.9.2 Prévoir des vérifications de la sécurité des sites Web pour déterminer les vulnérabilités et y remédier. Nous recommandons que l'application Web comprenne des mesures de sécurité pour prévenir les dix plus importants problèmes de sécurité (OWASP), c'est-à-dire : injection, authentification de mauvaise qualité, exposition de données sensibles, entités externes XML, contrôles d'accès défaillants, mauvaise configuration de sécurité, injection de code indirecte, désérialisation non sécurisée, utilisation de composants avec des vulnérabilités connues et supervision et journalisation insuffisantes.

3.2.9.3 Mettre votre site Web ou votre logiciel à jour régulièrement.

3.2.9.4 Installer des modules de sécurité et s'assurer qu'ils sont à jour.

3.2.9.5 Utiliser un système de sauvegarde pour votre site Web.

3.2.9.6 Établir une authentification par mot de passe ou une clé d'authentification publique et privée.

3.2.9.7 Établir des mots de passe sécuritaires et les changer régulièrement.

3.2.9.8 Utiliser une authentification à deux facteurs pour l'accès au site Web.

3.2.9.9 Créer des niveaux d'accès, limiter l'accès à des parties précises du site Web qui doivent être utilisées pour effectuer les tâches quotidiennes, privilège minimal.

3.2.9.10 Déployer un pare-feu d'applications Web.

3.2.9.11 Choisir un fournisseur d'hébergement Web qui offre une surveillance réseau en tout temps et une protection pare-feu pour bloquer toute menace connue.

3.2.9.12 Utiliser les pratiques exemplaires du Secure Software Development Framework pour neutraliser les risques des vulnérabilités des logiciels conformément à la publication du livre blanc du NIST (https://doi.org/10.6028/NIST.CSWP.04232020) [CSWP.04232020].

3.2.9.13 Obtenir les certifications et les attestations appropriées pour la conformité si les applications Web et les interfaces de programmation d'application normalisées traiteront des données sensibles, comme des données financières (PCI DSS), des données sur les soins de santé (HIPAA) et les renseignements permettant d'identifier une personne pour s'assurer qu'elles sont protégées (chiffrées) en cours d'utilisation, en transit et au repos.

3.2.10 Journalisation et vérification. La fonction de journalisation du système d'exploitation doit être activée, et les administrateurs du SI doivent examiner les fichiers journaux au moins une fois par trimestre ou chaque fois qu'ils soupçonnent une compromission. Cet examen doit porter notamment sur les ouvertures de session réussies et infructueuses, sur les modifications non autorisées apportées au matériel, au micrologiciel et aux logiciels du système, sur les comportements inhabituels du système, sur les perturbations imprévues des systèmes ou des services, sur les erreurs du système, etc. Les administrateurs système doivent être les seuls à pouvoir modifier ou supprimer les fichiers journaux et uniquement après en avoir été autorisés par l'ASE ou l'ARSE. Les IPO relatives au SI doivent préciser la fréquence et la méthode d'examen des fichiers journaux du système d'exploitation.

3.3 Équipement de TI

3.3.1 Inventaire de l'équipement. L'entrepreneur doit tenir à jour une liste de tout l'équipement qui constitue le SI. Celle-ci doit fournir, à tout le moins, la description de l'équipement ainsi que la marque, le modèle et la quantité de celui-ci. À la demande du PSC de SPAC et de l'officier de projet du MDN, cette liste doit leur être transmise.

3.3.2 Modifications apportées à l'équipement de TI. L'entrepreneur doit informer le PSC de SPAC et l'officier de projet du MDN de tout changement important apporté à l'équipement de TI du SI.

3.3.3 Technologie Bluetooth. Il est formellement interdit d'utiliser la technologie Bluetooth avec l'équipement de TI du SI. L'utilisation de la technologie Bluetooth dans la zone de travail ou la zone de travail temporaire où est situé le SI est strictement interdite, sauf le cas d'appareils médicaux approuvés. L'ASE doit être avisé de tout appareil médical Bluetooth utilisé à proximité du SI et doit autoriser par écrit l'utilisation d'un tel appareil.

3.3.4 Wi-Fi/sans fil. Il est permis d'utiliser des capacités sans fil ou Wi-Fi dans le cadre du SI, si les conditions suivantes sont respectées.

3.3.4.1 Les capacités sans fil ou Wi-Fi peuvent être utilisées aux installations de l'entrepreneur dans les conditions suivantes.

3.3.4.1.1 Toute connexion Wi-Fi ou sans-fil au SI doit être protégée par chiffrement. L'utilisation du protocole WPA2 est recommandée; le chiffrement minimal de 128-bits est obligatoire; le chiffrement de 256-bits est fortement encouragé.

3.3.4.1.2 L'entrepreneur doit établir des restrictions d'utilisation, y compris des mécanismes de contrôle de l'accès. Seul le personnel autorisé aura des comptes sur la connexion Wi-Fi ou sans fil.

3.3.4.1.3 Les pratiques exemplaires énoncées dans la publication du CCC, Annexe 2 – Conception de haut niveau – Connexion utilisateur sans fil/réseau câblé (ITSG-41), doivent être respectées.

3.3.4.1.4 La modification des réglages Wi-Fi ou sans fil n'est pas autorisée au niveau utilisateur. Toute modification doit être réalisée par les administrateurs de système après avoir obtenu l'accord écrit de l'officier de projet du MDN.

3.3.4.2 Les exigences sans fil et Wi-Fi des employés de l'entrepreneur qui travaillent à distance (employés effectuant des activités de télétravail ou d'informatique mobile) sont présentées dans la section 2 ci-dessus, au paragraphe « Télétravail et informatique mobile ».

3.3.4.3 Toute capacité Wi-Fi ou sans fil utilisée pour stocker, traiter ou produire des renseignements exclusifs dans le cadre du présent contrat doit d'abord être inspectée et autorisée par le PSC de SPAC.

3.3.5 Technologie infonuagique. L'utilisation de technologie infonuagique publique ou tierce pour stocker, traiter et produire des renseignements exclusifs est autorisée selon les conditions suivantes :

3.3.5.1 Seuls les services infonuagiques de logiciel-service (SaaS) et de système GSM seront utilisés.

3.3.5.1.1 Les renseignements exclusifs du contrat ne doivent pas être stockés à l'aide d'une technologie infonuagique tierce sans qu'elle utilise des contrôles de sécurité démontrés mis en œuvre par le fournisseur de services infonuagiques applicables, conformément aux publications gouvernementales suivantes :

3.3.5.1.1.1 Orientation sur l'utilisation sécurisée des services commerciaux d'informatique en nuage : Avis de mise en œuvre de la Politique sur la sécurité (https://www.canada.ca/fr/gouvernement/systeme/gouvernement-numerique/innovations-gouvernementales-numeriques/services-informatique-nuage/orientation-utilisation-securisee-services-commerciaux-informatique-nuage-amops.html)

3.3.5.1.1.2 Guide de sélection du nuage approprié du gouvernement du Canada (https://www.canada.ca/fr/gouvernement/systeme/gouvernement-numerique/innovations-gouvernementales-numeriques/services-informatique-nuage/gouvernement-canada-guide-selection-nuage-approprie.html)

3.3.5.1.1.3 Approche et procédures de gestion des risques à la sécurité de l'informatique en nuage du gouvernement du Canada (https://www.canada.ca/fr/gouvernement/systeme/gouvernement-numerique/innovations-gouvernementales-numeriques/services-informatique-nuage/approche-procedures-gestion-risques-securite-informatique-nuage.html)

3.3.5.1.1.4 Profil des mesures de sécurité pour les services du GC fondés sur l'informatique en nuage (https://www.canada.ca/fr/gouvernement/systeme/gouvernement-numerique/innovations-gouvernementales-numeriques/services-informatique-nuage/profil-controle-securite-services-ti-fondes-information-nuage.html)

3.3.5.1.1.5 Considérations relatives à l'utilisation de la cryptographie dans les services d'informatique en nuage commerciaux du gouvernement du Canada (https://www.canada.ca/fr/gouvernement/systeme/gouvernement-numerique/innovations-gouvernementales-numeriques/services-informatique-nuage/consideration-utilisation-crrptographie-services-informatique-nauge.html)

3.3.5.1.2 Tous les aspects de l'utilisation de l'infonuagique et de la technologie infonuagique par l'entrepreneur doivent d'abord être validés, évalués et autorisés soit par le ministère local (Dir Sécur) ou le Centre de la sécurité des télécommunications.

3.3.5.1.3 L'entrepreneur doit démontrer que les mesures sont conformes aux exigences énoncées dans les certifications et les rapports de vérification suivants en présentant, sur demande, des rapports d'évaluation ou des certifications de tierce partie indépendante ou des preuves précises de mise en œuvre de contrôles pour le niveau de service infonuagique (p. ex., IaaS, PaaS, SaaS) au sein des services infonuagiques, y compris : la norme ISO/IEC 27001 ou SOC 2 de type II et l'autoévaluation selon la matrice des contrôles infonuagiques de la Cloud Security Alliance.

3.3.5.1.4 En plus des exigences ci-dessus, l'entrepreneur doit répondre aux exigences décrites dans le calendrier 1 des obligations de sécurité relatives aux TI infonuagiques Protégé A ou s'y familiariser.

3.3.6 Diagramme de la topologie. L'entrepreneur doit fournir sur demande un diagramme de la topologie du SI au PSC de SPAC ou à l'officier de projet du MDN. Il doit consister en une conception de système de haut niveau et inclure tous les liens technologiques avec d'autres entités ainsi que les connexions à d'autres réseaux ou systèmes, le cas échéant.

3.3.7 Maintenance et élimination de l'équipement de TI. Lors de la maintenance et de l'élimination de tout équipement de TI utilisé pour stocker, traiter et créer des renseignements de nature exclusive (p. ex., des postes de travail, serveurs, imprimantes, traceurs, scanneurs, photocopieurs et des appareils et imprimantes multifonctions), on verra à suivre les directives fournies dans la section « Élimination » ci-dessous.

3.4 Autorisation et contrôle de l'accès

3.4.1 Liste du personnel autorisé. L'entrepreneur doit tenir à jour une liste des personnes autorisées qui ont accès au SI. Celle-ci doit être mise à jour en cas de changement du personnel ou des renseignements relatifs à une personne figurant dans la liste. Cette dernière doit inclure, à tout le moins, les données suivantes :

3.4.1.1 le nom de la personne;

3.4.1.2 le niveau d'habilitation de sécurité approuvé de la personne;

3.4.1.3 la date d'expiration de l'habilitation de sécurité de la personne;

3.4.1.4 le type de compte (p. ex., utilisateur, grand utilisateur, lecteur du journal des événements, administrateur).

3.4.2 Comptes système

3.4.2.1 Il faut créer un compte administrateur individuel pour chaque administrateur système. Si une personne a besoin à la fois d'un accès administrateur et d'un accès utilisateur courant, elle doit posséder deux comptes distincts sur le SI. Les comptes d'administrateur ne doivent pas être utilisés pour les opérations quotidiennes ou les questions non administratives.

3.4.2.2 Un compte d'utilisateur doit être créé pour chaque utilisateur; chaque compte doit comporter un nom ou identificateur exclusif. Ce nom ou cet identificateur ne peut pas être utilisé par tout autre détenteur d'un compte pour la durée de vie complète du système. Il faut configurer le compte individuel de façon à n'offrir que des privilèges limités. De plus, il ne doit permettre l'accès qu'aux fichiers et aux dossiers dont l'utilisateur a besoin dans la réalisation de ses tâches.

3.4.2.3 Le SI ne doit contenir :

3.4.2.3.1 aucun compte générique;

3.4.2.3.2 aucun compte d'invité;

3.4.2.3.3 aucun compte temporaire;

3.4.2.3.4 quelque compte partagé que ce soit.

3.4.3 Mots de passe

3.4.3.1 Chaque compte doit être protégé par un mot de passe dont la complexité est renforcée. Ainsi, le mot de passe doit, à tout le moins :

3.4.3.1.1 se composer d'au moins huit (8) caractères;

3.4.3.1.2 satisfaire à trois des quatre critères suivants pour sa composition :

- au moins une lettre majuscule (A à Z),

- au moins une lettre minuscule (a à z),
- au moins un chiffre (0 à 9),
- au moins un caractère spécial (p. ex., !, $, # et %);

3.4.3.1.3 avoir une durée de vie limitée, soit un minimum de 1 jour et un maximum de 90 jours;

3.4.3.1.4 être différent des dix (10) mots de passe précédents utilisés;

3.4.3.1.5 se verrouiller après quatre (4) tentatives de connexion infructueuses.

3.4.3.2 Tout mot de passe utilisé pour accéder au SI :

3.4.3.2.1 doit être changé lorsque l'utilisateur se connecte la première fois;

3.4.3.2.2 doit être changé lorsqu'on en soupçonne la compromission;

3.4.3.2.3 être différent des autres mots de passe de l'utilisateur pour accéder aux autres SI du contrat W6369-22-A009 Modification 1;

3.4.3.2.4 ne doit pas être enregistré ou mémorisé par le système d'exploitation ou toute application à laquelle ce dernier accède;

3.4.3.2.5 ne jamais être communiqué à qui que ce soit.

3.4.3.3 Il faut changer le mot de passe d'administrateur local d'origine dans tout l'équipement de TI formant le SI; on ne doit pas utiliser les mots de passe par défaut des fournisseurs.

3.4.3.4 Lorsque le mot de passe de l'administrateur local est changé, il doit être communiqué à tous les membres du personnel pertinents (techniciens du soutien informatique, administrateurs du système, etc.), qui doivent le protéger en fonction du niveau de sensibilité le plus élevé des données traitées par le système. Il doit être consigné sur papier et placé dans une enveloppe scellée portant sur son rabat la signature de l'ASE, de son remplaçant ou de l'administrateur du système, ainsi que la date courante. L'enveloppe doit être rangée dans un contenant verrouillé approuvé et protégé en fonction du niveau de sensibilité le plus élevé des données traitées par le système auquel le mot de passe donne accès.

3.4.4 Liste de contrôle d'accès au SI. Tous les éléments de réseau (physiques ou virtuels) du SI doivent être surveillés et accessibles (p. ex., au moyen de la liste de contrôle d'accès ou d'Active Directory) uniquement par le personnel autorisé.

3.4.5 Autorisation et contrôle d'accès dans les IPO. Les IPO relatives au SI doivent inclure un processus d'autorisation et de contrôle d'accès décrivant le processus d'ajout, de désactivation et de suppression des comptes utilisateur.

3.5 Supports informatiques

3.5.1 Élimination des supports de TI. Pendant toute la durée du contrat, tous les supports de TI utilisés pour stocker, traiter et créer des renseignements de nature exclusive doivent être éliminés conformément à la section « Élimination » du présent document.

3.5.2 Retrait des supports de TI. Dans les cas de soutien, de maintenance ou de remplacement du matériel, **aucun support informatique contenant des renseignements exclusifs** (p. ex., disques durs internes ou supports informatiques amovibles) ne sera fourni à tout fournisseur externe, fournisseur de services ou autre membre du personnel non autorisé ou mis à sa disposition.

3.5.3 Identification des supports de TI. Tous les supports de TI (p. ex., disques durs internes, amovibles ou externes, CD, DVD et clés USB) utilisés pour stocker, traiter et créer des renseignements de nature exclusive doivent satisfaire aux critères suivants :

3.5.3.1 ils doivent servir uniquement aux fins du présent contrat (aucun support amovible ne sera utilisé dans le SI pour tout transfert de données du contrat W6369-22-A009 Modification 1);

3.5.3.2 ils doivent avoir un identificateur exclusif afin d'en assurer un contrôle et un suivi adéquats;

3.5.3.3 ils doivent être identifiés et répertoriés comme suit :

3.5.3.3.1 type de support (p. ex., CD, DVD et clé USB),

3.5.3.3.2 niveau de sensibilité des renseignements,

3.5.3.3.3 mise en garde relative à la possibilité de diffusion (le cas échéant),

3.5.3.3.4 modèle et numéro de série (le cas échéant),

3.5.3.3.5 identificateur exclusif.

3.5.3.4 porter des étiquettes indiquant :

3.5.3.4.1 le niveau de confidentialité le plus élevé des données contenues,

3.5.3.4.2 le ministère fédéral (dans ce cas-ci, le MDN),

3.5.3.4.3 le numéro du contrat,

3.5.3.4.4 son identifiant exclusif.

S'il est impossible d'apposer une étiquette directement sur le support, il faut employer d'autres moyens (p. ex., une ficelle).

3.5.4 Protection des supports de TI. Tous les supports informatiques doivent être protégés en fonction du niveau de sensibilité le plus élevé des données qu'ils contiennent. Lorsqu'on ne les utilise pas, tous les supports informatiques amovibles, y compris les supports défaillants, ceux ayant un cycle de vie et ceux pour utilisation à long terme (p. ex., les supports de sauvegarde),

doivent être verrouillés dans un contenant sécurisé approuvé en fonction du niveau de sensibilité des données qu'ils contiennent.

3.5.5 Journalisation relative aux supports de TI amovibles. L'emplacement de tous les supports de TI amovibles doit faire l'objet d'un suivi et d'un contrôle au moyen d'un journal. Celui-ci doit contenir, à tout le moins, les renseignements suivants :

3.5.5.1 type de support (p. ex., CD, DVD, clé USB, disque dur amovible et bande de sauvegarde);

3.5.5.2 identificateur exclusif;

3.5.5.3 date et heure à laquelle le support a été retiré de son coffre de sécurité approuvé par le GC;

3.5.5.4 nom ou initiales et signature de la personne ayant emprunté le support;

3.5.5.5 date et heure à laquelle le support a été retourné dans son coffre de sécurité approuvé par le GC;

3.5.5.6 nom ou initiales et signature de la personne ayant retourné le support.

3.5.6 Poste de travail isolé. Le SI n'a pas à interagir avec des sources non fiables (p. ex., Internet, un autre réseau et le support de TI amovible d'une autre source), qui nécessite que l'entrepreneur fournisse un poste de travail isolé autonome.

3.6 Impression et reproduction de documents

3.6.1 Autorisation d'impression et de reproduction. L'entrepreneur :

3.6.1.1 n'est pas autorisé à imprimer et à reproduire dans ses installations les renseignements de nature exclusive;

3.6.1.2 n'est pas autorisé à utiliser des services d'impression et de reproduction à l'externe.

3.6.1.3

Le recours à l'un de ces services pour l'impression et la reproduction de renseignements de nature exclusive doit d'abord être approuvé par le PSC de SPAC et l'officier de projet du MDN.

3.6.2 Disques durs d'appareils d'impression et de reproduction. Les appareils utilisés pour reproduire des renseignements de nature exclusive (p. ex., des imprimantes, traceurs, scanneurs, photocopieurs et appareils et imprimantes multifonctions) peuvent être équipés de disques durs internes.

3.6.3 Connexions imprimantes. À moins que le SI ne soit configuré comme segment du réseau d'entreprise de l'entrepreneur, les imprimantes, traceurs, scanneurs, photocopieurs et appareils et imprimantes multifonctions doivent tous être connectés au SI. La connexion à d'autres appareils ou réseaux est strictement interdite.

3.6.4 Connexion de lignes téléphoniques. Il est strictement interdit de connecter des lignes téléphoniques à des appareils et imprimantes multifonctions utilisés pour traiter des renseignements de nature exclusive.

3.6.5 Reproduction de renseignements particulièrement sensibles. L'officier de projet du MDN doit approuver au préalable l'impression et la reproduction de renseignements de nature exclusive particulièrement sensibles de chaque document; si cette activité est approuvée, chaque copie doit se voir attribuer un identificateur exclusif afin d'en assurer un contrôle et un suivi adéquats.

3.7 Récupération

3.7.1 Sauvegardes du SI. Les renseignements exclusifs doivent faire l'objet de sauvegardes régulières, au moins une fois par semaine, lesquelles doivent être conservées en sécurité dans un emplacement distant (c.-à-d. un emplacement différent qui ne risque pas d'être touché par le même incident, comme un feu ou une inondation, qui frapperait l'emplacement principal). Si l'entrepreneur ne dispose pas d'un emplacement distant pour conserver les sauvegardes, des arrangements peuvent être pris avec l'officier de projet du MDN. Si les sauvegardes doivent être conservées par une entreprise privée différente de celle de l'entrepreneur, cela doit faire l'objet d'un contrat de sous-traitance. Les IPO relatives au SI doivent préciser les détails relatifs à la fréquence, à la méthodologie et au stockage des sauvegardes.

3.7.2 Mise à l'essai des sauvegardes. Les sauvegardes du SI doivent faire l'objet d'essais réguliers. Les IPO relatives au Si doivent fournir tous les renseignements nécessaires ayant trait à la fréquence de ces vérifications, à la méthode employée et au signalement des erreurs relevées.

3.7.3 Plan de reprise après sinistre. L'entrepreneur doit élaborer et documenter un plan de reprise après sinistre du SI. Ce plan doit préciser les détails de la reprise, du rétablissement, ainsi que de la fréquence et de la méthodologie des essais.

3.8 Élimination

3.8.1 Élimination des supports de TI. Avant l'élimination des supports informatiques utilisés dans le cadre du contrat, l'entrepreneur doit suivre les directives du paragraphe 3.8.2, Nettoyage et destruction des supports de TI. Cela comprend les supports informatiques défectueux, arrivés en fin de vie et devenus inutiles. L'élimination des supports informatiques doit faire l'objet d'un suivi au moyen d'un certificat de destruction. L'entrepreneur doit conserver un exemplaire de tout document ayant trait à l'élimination des supports informatiques comme preuve qu'il a procédé conformément aux directives. L'élimination de biens et de renseignements classifiés doit être consignée dans un certificat de destruction, dont une copie doit être envoyée au PSC de SPAC par courriel à l'adresse suivante : tpsgc.dgsssiprojetintl-dobissintlproject.pwgsc@tpsgc-pwgsc.gc.ca.

3.8.2 Nettoyage des supports de TI. Le nettoyage et l'élimination de tous les supports de TI sur place sont autorisés aux installations de l'entrepreneur, sous condition que l'entrepreneur respecte les consignes de nettoyage et d'élimination des supports de nature très délicate, conformément à la publication *Nettoyage des supports de TI (ITSP.40.006) v2* du CST et le chapitre 6 du manuel de la sécurité des contrats, *6.10 Destruction des documents*. Les dispositions peuvent être prises avec le PSC de SPAC pour l'élimination des supports de TI si l'entrepreneur ne possède pas les moyens requis pour l'effectuer.

3.8.3 Retour des renseignements, du matériel et de l'équipement fournis par le gouvernement. Les renseignements, le matériel et l'équipement fournis par le gouvernement demeureront la propriété du MDN et ne doivent pas être distribués à l'extérieur de l'équipe de l'entrepreneur du contrat, sauf avec l'approbation de l'officier de projet. Les renseignements, le matériel et l'équipement doivent être retournés à l'officier de projet du MDN à l'achèvement du contrat.

3.8.4 Procédures préalables au retrait de l'équipement de TI. S'il est nécessaire de procéder à la maintenance et à l'élimination de l'équipement de TI, les procédures ci-dessous doivent être respectées avant de retirer tout équipement de TI utilisé pour stocker, traiter et créer des renseignements de nature exclusive; ces procédures s'appliquent à tout équipement de TI renfermant des supports de TI (p. ex., des serveurs, postes de travail, imprimantes, traceurs, scanneurs et appareils et imprimantes multifonctions).

3.8.4.1 Il faut retirer et éliminer tous les appareils de mémoire non volatile (p. ex., disques durs internes, amovibles et externes) de la manière indiquée dans la présente section.

3.8.4.2 La mémoire volatile (p. ex., mémoire vive, DRAM, SRAM) doit être épurée en coupant toute alimentation pendant au moins 24 heures consécutives. L'entrepreneur doit s'assurer qu'il n'y a pas de courant dans la mémoire (p. ex., aucune pile interne ni connexion à un autre appareil). En cas de doute quant à l'élimination complète de l'alimentation dans la mémoire volatile de l'équipement utilisé pour stocker, traiter et créer des renseignements de nature exclusive hautement sensibles, l'entrepreneur verra à retirer cette mémoire et à la faire détruire.

3.8.4.3 Il faut enlever tout autocollant ou marque de sécurité sur l'appareil en rapport avec le contrat ou le SI.

National Defence | Défense nationale

National Defence Headquarters
Ottawa, Ontario
K1A 0K2

Quartier général de la Défense nationale
Ottawa (Ontario)
K1A 0K2

APPENDICE 3 DE L'ANNEXE «C» – OBLIGATIONS DE SÉCURITÉ RELATIVES AUX TI INFONUAGIQUES

Pour les obligations de sécurité relatives aux TI infonuagiques Protégé A

Calendrier 1 du document sur les exigences relatives à la sécurité des TI pour le contrat W6369-22-A009 Modification 1

1. Généralités

1.1 *Objectif*

L'objectif de ce calendrier est d'établir les obligations de l'entrepreneur relatives à la gestion appropriée des données du MDN, y compris la protection contre tout accès et toute modification ou exfiltration non autorisés, conformément à l'accord, ce calendrier et les mesures de sécurité de l'entrepreneur (collectivement les « **obligations de sécurité** »). De plus, l'entrepreneur doit démontrer qu'il continue de répondre aux mêmes exigences relatives à la sécurité et à la configuration qui ont été précédemment évaluées et approuvées par le CCC.

Le présent document décrit les exigences relatives à la sécurité des TI du MDN pour le traitement, la production ou le stockage électroniques des données du Canada, y compris et jusqu'à concurrence du niveau Protégé A.

La sécurité repose sur diverses couches de protection. En d'autres termes, les exigences relatives à la sécurité des TI, lorsqu'elles sont respectées, permettent de protéger l'information efficacement seulement si d'autres mesures et politiques de sécurité les sous-tendent. On ne doit réaliser des travaux sous-traités qu'après avoir mis en œuvre des mesures de protection physiques, du personnel, des procédures, de l'information et de sécurité des TI.

1.2 *Transfert des obligations en matière de sécurité*

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

1.3 *Gestion du changement*

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

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

2. Reconnaissance

Les parties reconnaissent que :

(a) les données du MDN sont assujetties 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 données du MDN;

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

(d) les obligations en matière de sécurité s'appliquent jusqu'au niveau Protégé A/Intégrité moyenne/Disponibilité moyenne ou Blessure moyenne, sauf indication contraire.

3. Sécuriser les données du ministère de la Défense nationale (MDN)

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

4. Rôles et responsabilités liés à la sécurité

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

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

5. Assurance tierce : Attestations et rapports

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

(2) L'entrepreneur doit démontrer que les mesures sont conformes aux exigences énoncées dans les certifications et les rapports de vérification suivants en présentant, sur demande, des rapports d'évaluation ou des certifications de tierce partie indépendante ou des preuves précises de mise en œuvre de contrôles pour chaque niveau de service (p. ex., IaaS, PaaS, SaaS) au sein des services infonuagiques, y compris :

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

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

(c) réaliser une autoévaluation selon la matrice des contrôles infonuagiques de la Cloud Security Alliance en utilisant la plus récente version téléchargée à partir de https://cloudsecurityalliance.org/.

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

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

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

(6) L'entrepreneur devra maintenir des contrôles de sécurité qui appuient la conformité avec la norme ISO 27001 ou SOC 2 de type II pour la période du contrat. L'entrepreneur doit fournir, au moins une fois par année et rapidement à la demande du responsable de projet du MDN, tous les rapports ou les preuves de mise en œuvre de contrôles pouvant être raisonnablement exigés pour démontrer la conformité de l'entrepreneur ou que celui-ci possède les certifications actuelles.

(7) L'autoévaluation selon la matrice des contrôles infonuagiques de la Cloud Security Alliance doit être mise à la disposition du MDN.

6. Vérification de la 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 données du MDN comme suit :

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

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

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

(2) Chaque vérification donnera lieu à la production d'un rapport de vérification qui doit être mis à la disposition du responsable de projet du MDN. Le rapport de vérification doit indiquer clairement toutes les constatations importantes faites par le vérificateur tiers.

L'entrepreneur doit, à ses frais, corriger rapidement et à la satisfaction du vérificateur les problèmes et les lacunes soulevés dans tout rapport de vérification.

(3) À la demande du responsable de projet du MDN, l'entrepreneur ou un sous-traitant peut fournir des preuves supplémentaires, y compris des plans de sécurité du système, des conceptions ou des documents d'architecture qui fournissent une description complète du système, afin d'achever les rapports de certification et de vérification décrits à la section 5, Assurance d'une tierce partie, et de démontrer la conformité de l'entrepreneur avec les certifications requises de l'industrie.

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

(1) L'entrepreneur doit respecter les exigences de sécurité sélectionnées dans le Profil de contrôle de sécurité pour les services des TI du GC fondés sur l'informatique en nuage pour les renseignements classés « Protégé A/Intégrité moyenne/Disponibilité moyenne » (https://www.canada.ca/fr/gouvernement/systeme/gouvernement-numerique/innovations-gouvernementales-numeriques/services-informatique-nuage/profil-controle-securite-services-ti-fondes-information-nuage.html) selon la portée des services infonuagiques offerts par l'entrepreneur. La conformité doit être démontrée sur demande par la mise en correspondance des contrôles de sécurité avec les certifications de l'industrie applicables énoncées ci-dessous, puis validée au moyen d'évaluations de tiers indépendants.

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

L'entrepreneur doit lancer le processus officiel d'évaluation du CCC et s'engager à réaliser le programme sans retard inutile. L'entrepreneur doit fournir les documents suivants au fur et à mesure qu'ils sont disponibles :

(i) Une copie de la lettre de confirmation stipulant qu'il a intégré le programme;
(ii) Une copie du rapport d'évaluation le plus récent fourni par le CCC;
(iii) Une copie du rapport sommaire le plus récent fourni par le CCC.

L'entrepreneur qui souhaite en savoir plus sur le processus d'évaluation des TI du CCC doit communiquer avec le service à la clientèle du CCC.

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

8. Protection des données

(1) L'entrepreneur doit fournir au MDN la capacité de :

(a) mettre en œuvre le chiffrement des données au repos pour les services infonuagiques qui hébergent les données du MDN dans les cas où le chiffrement des données au repos demeure en vigueur, ininterrompu et actif à tout moment, même dans l'éventualité de panne d'équipement ou de technologie, conformément à l'article 14, Protection cryptographique;

(b) transmettre les données du MDN de manière sécuritaire qui offre au GC et au MDN la possibilité de mettre en œuvre le chiffrement des données en transit pour toutes les transmissions des données du MDN, conformément à l'article 14, Protection cryptographique et à l'article 21, Sécurité des réseaux et des communications.

(2) L'entrepreneur doit :

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

(b) prendre des mesures raisonnables pour s'assurer que le personnel de l'entrepreneur n'a pas de droits d'accès permanents ou continus aux données du MDN, et l'accès est limité au personnel de l'entrepreneur doté du besoin de savoir, notamment les ressources qui offrent un soutien technique ou au MDN, sur approbation du responsable de projet du MDN.

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

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

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

9. Isolement des données

(1) L'entrepreneur doit mettre en place des contrôles afin d'assurer un isolement approprié des ressources, afin que les données du MDN ne se retrouvent pas mêlées à celles d'autres locataires sans contrôle à cet effet, et ce, pendant l'utilisation, le stockage ou le transfert, et dans tous les aspects des fonctions et de l'administration du système des services infonuagiques et de l'infrastructure de l'entrepreneur. Cela nécessite la mise en œuvre de contrôles d'accès et la mise en place d'une séparation logique ou physique appropriée pour soutenir :

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

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

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

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

10. Emplacement des données

(1) L'entrepreneur doit avoir la capacité de stocker et de protéger les données du MDN, au repos, y compris les données sauvegardées ou conservées aux fins de redondance. 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 l'article 30 pour la sécurité physique (centre de données ou installations);

b. Garantit l'impossibilité de trouver les données du MDN en particulier sur des supports physiques;

c. Emploie le chiffrement pour s'assurer qu'aucune donnée n'est écrite sur disque sous une forme non chiffrée, conformément à l'article 14, Protection cryptographique.

(2) L'entrepreneur doit certifier que la prestation et l'approvisionnement des services infonuagiques en vertu du présent contrat proviennent :

a. de pays de l'Organisation du Traité de l'Atlantique Nord (OTAN) [https://www.nato.int/cps/fr/natohq/nato_countries.htm];

b. de pays de l'Union européenne (UE) [https://europa.eu/european-union/about-eu/countries_fr] ou de pays avec lesquels le Canada a un accord international ou bilatéral en matière de sécurité industrielle. Dans le cadre du Programme de sécurité des contrats, des accords internationaux bilatéraux en matière de sécurité industrielle ont été conclus avec les pays énumérés sur le site Web https://www.tpsgc-pwgsc.gc.ca/esc-src/international-fra.html de SPAC. La liste est mise à jour périodiquement.

(3) L'entrepreneur doit avoir la capacité pour le MDN d'isoler les données du MDN hébergées par les services infonuagiques des centres de données situés géographiquement au Canada ou à l'extérieur du Canada.

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

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

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

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

11. Transfert et récupération des données

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

(a) Extraire toutes les données du MDN en ligne, pseudodirectes et hors ligne, y compris, sans toutefois s'y limiter, les bases de données, le stockage d'objets et de fichiers, les configurations de système, les journaux d'activités infonuagiques, les codes source hébergés dans un référentiel de codes du MDN et les configurations réseau, de sorte que le MDN puisse se servir de ces instructions pour effectuer la migration d'un environnement à un autre;

(b) Effectuer le transfert sécurisé de toutes les données du MDN, y compris les données de contenu et les métadonnées associées, dans un format lisible et utilisable par machine, conformément à l'article 9 des Lignes directrices sur les formats de fichier à utiliser pour transférer des ressources documentaires à valeur continue de Bibliothèque et Archives Canada (https://www.bac-lac.gc.ca/fra/services/gestionressources-documentaires-gouvernement/lignes-directrices/Pages/lignes-directrices-formatsfichier-transferers-ressources-documentaires.aspx).

12. Supports de TI

(1) Tout au long du présent contrat, il faut éliminer tous les supports informatiques utilisés pour traiter, produire ou stocker des renseignements du MDN conformément aux procédures décrites dans la section 13, Disposition et remise des données.

(2) Dans les cas de soutien, de maintenance ou de remplacement du matériel, **aucun support informatique contenant des renseignements du MDN** (p. ex., disques durs internes ou supports informatiques amovibles) ne sera fourni à tout fournisseur externe, fournisseur de services ou autre membre du personnel non autorisé ou mis à sa disposition.

(3) Tous les supports informatiques (p. ex., disques durs internes, amovibles ou externes, CD, DVD et clés USB) employés pour traiter, produire ou stocker des renseignements du MDN doivent :

(a) servir uniquement aux fins de ce contrat;

(b) avoir un identificateur exclusif afin d'en assurer un contrôle et un suivi adéquats;

(c) être identifiés et répertoriés comme suit :

(i) type de support (p. ex., CD, DVD et clé USB),

(ii) niveau de sensibilité des renseignements,

(iii) la restriction à la divulgation (s'il y a lieu),

(iv) le modèle et le numéro de série (s'il y a lieu);

(d) porter des étiquettes indiquant :

(i) le niveau de confidentialité le plus élevé des données contenues,

(ii) le ministère fédéral (dans ce cas--ci, le MDN),

(iii) le numéro du contrat,

(iv) son identifiant exclusif.

(e) S'il est impossible d'apposer une étiquette directement sur le support, il faut employer d'autres moyens (p. ex., une ficelle).

(f) Tous les supports informatiques doivent être protégés en fonction du niveau de sensibilité le plus élevé des données qu'ils contiennent. Lorsqu'on ne les utilise pas, tous les supports informatiques amovibles, y compris les supports défaillants, ceux ayant un cycle de vie et ceux pour utilisation à long terme (p. ex., les supports de sauvegarde), doivent être verrouillés dans un contenant sécurisé approuvé en fonction du niveau de sensibilité des données qu'ils contiennent.

(g) L'emplacement de tous les supports de TI amovibles doit faire l'objet d'un suivi et d'un contrôle au moyen d'un journal. Celui-ci doit contenir, à tout le moins, les renseignements suivants :

(i) type de support (p. ex., CD, DVD et clé USB);

(ii) identificateur exclusif;

(iii) date et heure à laquelle le support a été retiré;

(iv) le nom ou les initiales de la personne qui l'a emprunté;

(v) date et heure de retour du support;

(vi) le nom ou les initiales de la personne qui l'a retourné.

13. Disposition des dossiers et remise des dossiers au ministère de la Défense nationale (MDN)

(1) Élimination des supports de TI. Avant l'élimination des supports informatiques utilisés dans le cadre du contrat, l'entrepreneur doit suivre les directives du paragraphe 2, Nettoyage et destruction des supports de TI. Cela comprend les supports informatiques défectueux, arrivés en fin de vie et devenus inutiles. L'élimination des supports informatiques doit faire l'objet d'un suivi au moyen d'un certificat de destruction. L'entrepreneur doit conserver un exemplaire de tout document ayant trait à l'élimination des supports informatiques comme preuve qu'il a procédé conformément aux directives. L'élimination de biens et de renseignements classifiés doit être consignée dans un certificat de destruction, dont une copie doit être envoyée au PSC de SPAC par courriel à l'adresse suivante : tpsgc.dgsssiprojetintl-dobissintlproject.pwgsc@tpsgc-pwgsc.gc.ca.

(2) Nettoyage des supports de TI. Le nettoyage et l'élimination de tous les supports de TI sur place sont autorisés aux installations de l'entrepreneur, sous condition que l'entrepreneur respecte les consignes de nettoyage et d'élimination des supports de nature très délicate, conformément à la publication *Nettoyage des supports de TI (ITSP.40.006) v2* du CST et le chapitre 6 du manuel de la sécurité des contrats, *6.10 Destruction des documents*.

(3) Les dispositions peuvent être prises avec le PSC de SPAC pour l'élimination des supports de TI si l'entrepreneur ne possède pas les moyens requis pour l'effectuer.

(4) Retour des renseignements, du matériel et de l'équipement fournis par le gouvernement. Les renseignements, le matériel et l'équipement fournis par le gouvernement demeureront la propriété du MDN et ne doivent pas être distribués à l'extérieur de l'équipe de l'entrepreneur du contrat, sauf avec l'approbation de l'officier de projet. Les renseignements, le matériel et l'équipement doivent être retournés à l'officier de projet du MDN à l'achèvement du contrat.

(5) S'il faut procéder à la maintenance ou à l'élimination du matériel informatique, on doit appliquer les procédures suivantes avant de retirer tout matériel informatique utilisé pour traiter, produire ou stocker les renseignements exclusifs. Ce processus s'applique à tout l'équipement de TI contenant des supports informatiques (p. ex., des serveurs, postes de travail, imprimantes, traceurs, numériseurs, appareils ou imprimantes multifonctions).

a. Il faut retirer et éliminer tous les dispositifs de mémoire non volatile (disques durs internes, amovibles et externes, etc.) conformément aux directives de la présente section.

b. La mémoire volatile (p. ex., mémoire vive, DRAM, SRAM) doit être épurée en coupant toute alimentation pendant au moins 24 heures consécutives. L'entrepreneur doit s'assurer qu'il n'y a pas de courant dans la mémoire (p. ex., aucune pile interne ni connexion à un autre appareil). S'il a quelque doute que ce soit concernant le retrait de l'alimentation à la mémoire volatile de l'équipement utilisé pour traiter, produire ou stocker des renseignements exclusifs de nature très délicate, l'entrepreneur doit retirer cette mémoire et la faire détruire.

c. Il faut enlever tout autocollant ou marque de sécurité sur l'appareil en rapport avec le contrat ou le SI.

14. Protection cryptographique

L'entrepreneur doit :

(a) configurer toute solution cryptographique qui est adoptée à l'égard des services et qui est utilisée dans le cadre de la mise en œuvre de mesures de protection de la confidentialité ou de l'intégrité ou encore d'un mécanisme d'authentification (p. ex., solutions liées au réseau privé virtuel, protocole TLS, modules logiciels, indicateurs de rendement clés et jetons d'authentification, le cas échéant), conformément aux algorithmes cryptographiques, tailles de clés de chiffrement et périodes de validité des clés approuvés par le CST;

(b) utiliser des algorithmes cryptographiques, des tailles de clés cryptographiques ainsi que des cryptopériodes qui ont été validés par le Programme de validation des algorithmes cryptographiques (http://csrc.nist.gov/groups/STM/cavp/), et spécifiés dans le document ITSP.40.111 Algorithmes cryptographiques pour l'information NON CLASSIFIÉ, PROTÉGÉ A et PROTÉGÉ B ou dans des versions subséquentes de ce document (https://cyber.gc.ca/fr/orientation/algorithmes-cryptographiques-linformation-non-classifie-protege-protege-b-itsp40111);

(c) s'assurer que la cryptographie validée selon la norme FIPS 140-2 ou plus récente est utilisée lorsqu'un chiffrement est nécessaire et qu'elle est mise en œuvre, configurée et exploitée dans un module cryptographique, validé par le Programme de validation des modules cryptographiques (https://cyber.gc.ca/fr/outils-services/programme-validation-modules-cryptographiques-pvmc), dans un mode approuvé ou autorisé afin de fournir un degré élevé de certitude que le module cryptographique validé FIPS 140-2 ou plus récente fournit les services de sécurité prévus de la manière prévue;

(d) s'assurer que tous les modules FIPS 140-2 ou 140-3 utilisés ont une certification active, à jour et valide. Les produits conformes ou validés selon la norme FIPS 140 auront un numéro de certificat.

15. Gestion des clés

L'entrepreneur doit fournir au responsable de projet du MDN un service de gestion des clés qui permet :

(a) la création ou la génération et la suppression des clés de cryptage par le GC;

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

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

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

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

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

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

16. Protection des points terminaux

(1) L'entrepreneur doit mettre en œuvre, gérer et surveiller les points d'accès sécurisés dotés de protection active par le système d'hébergement afin de prévenir les maliciels, les attaques et les abus conformément aux lignes directrices de configuration reconnues par l'industrie, comme celles du document NIST 800-123 (Guide to General Server Security [guide relatif à la sécurité générale des serveurs]), des points de référence du Center for Internet Security ou des produits certifiés du CST (https://www.cyber.gc.ca/fr/outils-services/criteres-communs/produits-certifies) ou d'une norme équivalente approuvée par écrit par le responsable de projet du MDN.

(2) L'entrepreneur doit mettre en œuvre un cycle de vie de développement de logiciels et de systèmes qui applique les principes d'ingénierie de la sécurité des systèmes d'information tout au long de leur cycle de vie et dans le développement de logiciels, de sites Web et de services. Ce cycle de vie doit être conforme aux normes et aux pratiques

exemplaires du secteur, comme : i) NIST, ii) ISO 27034, iii) ITSG-33, iv) SAFECode ou v) Open Web Application Security Project (OWASP) (p. ex., Application Security Verification Standard [ASVS]) ou une norme équivalente approuvée par le MDN par écrit. À la demande du MDN, l'entrepreneur doit fournir un document qui décrit le logiciel documenté de l'entrepreneur, ainsi que l'approche et le processus adoptés relativement au cycle de vie du développement du système.

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

(1) L'entrepreneur doit avoir la capacité pour le MDN 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 V3 (ou une version subséquente) du CST 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.

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

18. Fédération

(1) L'entrepreneur doit permettre au MDN 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, où les justificatifs et authentificateurs des utilisateurs du GC pour les services infonuagiques sont contrôlés uniquement par le MDN;

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

19. Gestion des accès privilégiés

(1) L'entrepreneur doit :

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

(b) restreindre et minimiser l'accès aux services infonuagiques;

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

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

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

(f) mettre en œuvre des politiques sur les mots de passe afin de protéger les justificatifs d'identité contre les attaques en ligne ou hors ligne et de détecter ces attaques en consignant et en surveillant des événements tels que (i) l'utilisation réussie des justificatifs d'identité, (ii) l'utilisation inhabituelle de ces derniers et (iii) l'accès et l'exfiltration de la base de données des mots de passe, conformément à la version 3 (ou aux versions ultérieures) de la norme 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 œuvre des mécanismes d'authentification multifactorielle pour authentifier les utilisateurs finaux ayant un accès privilégié, conformément à la norme ITSP.30.031 V3 du CST (ou à ses versions ultérieures) (https://cyber.gc.ca/fr/orientation/guide-sur-lauthentification-des-utilisateurs-dans-les-systemes-de-technologie-de);

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

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

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

(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) pour offrir le soutien et l'administration des services infonuagiques et de l'infrastructure de l'entrepreneur;

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

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

(2) L'entrepreneur doit fournir au responsable de projet du MDN un document qui décrit son approche et son processus pour la gestion et la surveillance des accès privilégiés aux services infonuagiques.

20. Gestion à distance

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

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

(b) employer des mécanismes cryptographiques pour protéger la confidentialité des séances d'accès à distance, conformément à l'article 14, Protection cryptographique;

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

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

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

(2) L'entrepreneur doit fournir au responsable de projet du MDN un document qui décrit son approche et son processus pour la gestion et la surveillance de l'administration à distance des services infonuagiques.

21. Sécurité des réseaux et des communications

(1) L'entrepreneur doit :

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

(b) employer des protocoles ainsi que des algorithmes et des certificats cryptographiques pris en charge et à jour, comme le décrivent les normes ITSP.40.062 (https://cyber.gc.ca/fr/orientation/conseils-sur-laconfiguration-securisee-des-protocoles-reseau-itsp40062) et ITSP.40.111 (https://cyber.gc.ca/fr/orientation/algorithmes-cryptographiques-pour-linformation-nonclassifie-protege-et-protege-b);

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

(d) permettre au MDN 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 du MDN.

22. Connexions dédiées

(1) Pour les niveaux IaaS, l'entrepreneur doit permettre au GC d'établir une connectivité privée redondante aux services infonuagiques. Cela comprend :

(a) l'établissement de la connectivité directement dans le Réseau étendu de la Défense ou par l'intermédiaire d'un emplacement approuvé par le gouvernement du Canada au sein des limites géographiques du Canada; n'est pas obligatoire pour le SI infonuagique Protégé A;

(b) la prestation de services complets de sauvegarde et de reprise après sinistre au moyen de la prise en charge des connexions redondantes à l'intérieur des centres de données de l'entrepreneur et entre ceux-ci;

(c) des liens de connectivité physique qui sont optiques et qui offrent un minimum de 10 Gb/s et l'option d'y ajouter des liens de jusqu'à 40 Gb/s, avec une connectivité facultative de 100 Gb/s;

(d) la prise en charge de la virtualisation et de locataires multiples pour tous les composants réseau;

(e) la prise en charge de protocoles de routage dynamiques (Border Gateway Protocol) pour toutes les connexions;

(f) la prise en charge de protocoles approuvés par le GC, qui sont décrits dans les documents suivants :

i. Conseils sur la configuration sécurisée des protocoles réseau (ITSP.40.062), section 3.1 (suites de chiffrement AES) [https://cyber.gc.ca/fr/orientation/conseils-sur-la-configuration-securisee-des-protocoles-reseau-itsp40062];
ii. ITSP.40.111 Algorithmes cryptographiques pour l'information Non classifié, Protégé A et Protégé B [https://cyber.gc.ca/fr/orientation/algorithmes-cryptographiques-linformation-non-classifie-protege-protege-b-itsp40111];

(g) fournir une description des emplacements de tous les centres de données où cette capacité est offerte;

23. Journalisation et vérification

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

(2) L'entrepreneur doit offrir au MDN la capacité d'exporter les journaux d'événements de sécurité pour les services infonuagiques utilisés, en appui aux opérations du gouvernement du Canada, y compris la surveillance des services infonuagiques, les preuves électroniques et les mises en suspens pour raisons juridiques.

(3) L'entrepreneur doit permettre au MDN d'examiner et d'analyser de manière centralisée les dossiers de vérification de multiples composants des services infonuagiques utilisés par le MDN. Ceci comprend la capacité du MDN :

(a) d'enregistrer et de détecter les événements de vérification tels que (i) les tentatives de connexion réussies ou non, (ii) la gestion des comptes, (iii) l'accès aux objets et changement de politique, (iv) les fonctions de privilèges et de suivi des processus, (v) les événements système, (vi) la suppression des données;

(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 autorisé, 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 MDN afin de permettre au MDN de surveiller et de gérer les événements à l'intérieur de ses frontières qui ont une incidence sur l'instance d'un service infonuagique IaaS, PaaS ou SaaS qui lui est rendu par l'entrepreneur ou un sous-traitant;

(d) de transmettre les événements et journaux des locataires du MDN 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.).

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

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

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

24. Surveillance continue

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

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

(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 infonuagiques, données et composants pertinents aux services infonuagiques IaaS, PaaS ou SaaS du MDN;

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

(f) répondre aux menaces et aux attaques contre les services infonuagiques du fournisseur, 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 infonuagiques de l'entrepreneur doivent permettre de copier les données des applications (IaaS, PaaS et SaaS) et le trafic réseau (IaaS et PaaS) du gouvernement du Canada dans les services infonuagiques hébergés et de les acheminer vers un emplacement prédéterminé (dans le nuage ou dans les locaux du gouvernement).

(3) Les services infonuagiques de l'entrepreneur doivent permettre au gouvernement du Canada de déployer et d'utiliser des logiciels de sécurité pour assurer la surveillance avancée et l'atténuation des cybermenaces pour les services infonuagiques du gouvernement et l'hôte géré par le gouvernement et la couche réseau, pour les composants gérés par le gouvernement seulement.

(4) Le MDN se réserve le droit d'inspecter, selon une fréquence et un calendrier que déterminera le responsable de la sécurité des TI du MDN, mais avec un préavis raisonnable et selon les contraintes des lois et des règlements applicables en matière de protection des renseignements personnels, chaque installation de l'entrepreneur servant au présent contrat, y compris les installations des fournisseurs d'infrastructures en sous-traitance, afin d'assurer la conformité aux exigences en matière de sécurité des TI énoncées dans le présent document ainsi qu'aux exigences et politiques du GC en matière de prévention, de détection, d'intervention et de reprise.

25. Gestion des incidents de sécurité

(1) Le processus d'intervention en cas d'incident de sécurité de l'entrepreneur pour les services infonuagiques doit comprendre un processus de gestion des incidents de sécurité des TI ainsi que des pratiques de soutien des activités de préparation, de détection, d'analyse, de confinement et de récupération. Cela comprend :

(a) un processus d'intervention en cas d'incident de sécurité publié et documenté aux fins d'examen par le MDN, qui est conforme à l'une des normes suivantes : i) ISO/IEC 27035:2011 Technologies de l'information – Techniques de sécurité – Management des incidents liés à la sécurité de l'information; ou ii) NIST SP800-612, Computer Security Incident Handling Guide; ou iii) Plan de gestion des événements de cybersécurité du gouvernement du Canada (https://www.canada.ca/fr/secretariat-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 fournisseurs de services si le MDN 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 MDN, y compris : (i) la portée des incidents de sécurité de l'information que l'entrepreneur doit signaler au MDN; (ii) le degré de divulgation des incidents de sécurité de l'information détectés et les réponses connexes; (iii) le délai cible de signalement des incidents de sécurité de l'information; (iv) la procédure de signalement et d'acheminement en cas d'incidents de sécurité; (v) les coordonnées des personnes-ressources pour le traitement des enjeux relatifs aux incidents de sécurité de l'information; (vi) tout recours applicable à certains incidents de sécurité de l'information;

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

(d) Cela permet uniquement aux représentants désignés du MDN autorisés (comme le Centre des opérations de sécurité de SPC) par le responsable technique :

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

(ii) 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 infonuagiques, y compris des procédures judiciaires et des mesures de protection pour la tenue d'une chaîne de possession.

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

(3) L'entrepreneur doit :

(a) collaborer avec le Centre des opérations de sécurité du MDN (p. ex., CCC, SOC ministériel) en ce qui concerne le confinement, l'élimination et la reprise en cas d'incident de sécurité, conformément au processus d'intervention en cas d'incident de sécurité;

(b) tenir un registre des violations de la sécurité comprenant une description de la violation de la sécurité, la durée, les conséquences de la violation, le nom de la personne ayant signalé la violation, et la personne à qui la violation a été signalée, et la procédure pour récupérer les données ou le service;

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

(5) Le MDN pourrait exiger des preuves judiciaires de la part de l'entrepreneur pour contribuer à une enquête du GC. L'entrepreneur consent à fournir de l'aide au GC dans la mesure du possible.

26. Intervention en cas d'incident de sécurité

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

(2) Si 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 MDN ou des données personnelles du MDN pendant le traitement par l'entrepreneur (chacun étant un « incident de sécurité ») et qu'il la relève, l'entrepreneur doit rapidement et sans tarder (i) informer le MDN de cet incident de sécurité; (ii) mener une enquête et fournir des renseignements détaillés au responsable de projet du MDN sur cet incident de sécurité; (iii) prendre les mesures raisonnables pour remédier aux causes et atténuer les dommages découlant de l'incident de sécurité.

27. Fuite d'information

(1) L'entrepreneur doit avoir un processus documenté qui énonce son approche en cas d'incident de fuite d'information. Le processus doit être harmonisé i) aux directives de la section IR-9 intitulée « Intervention en cas de fuite d'information » du document ITSG-33, ou ii) à une autre pratique exemplaire du secteur approuvée par écrit par le responsable de projet du MDN. Nonobstant ce qui précède, le processus d'intervention en cas de fuite d'information de l'entrepreneur doit comprendre, à tout le moins :

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

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

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

(2) L'entrepreneur doit fournir au responsable de projet du MDN un document qui décrit le processus d'intervention en cas de fuite d'information de l'entrepreneur.

28. Essais de sécurité et validation

(1) L'entrepreneur doit disposer d'un processus qui permet au MDN, sur demande et selon des conditions convenues, d'effectuer une analyse de vulnérabilité ou un essai de pénétration non perturbateur et non destructif visant la partie des composantes du MDN du service infonuagique dans l'environnement de l'entrepreneur.

(2) L'entrepreneur doit offrir la possibilité de mettre en place un outil libre-service de vérification de l'état de la sécurité, de la conformité ou un outil de notation qui permet de

mesurer la posture de sécurité des services infonuagiques applicables utilisés dans le cadre des services du MDN.

29. Filtrage de sécurité du personnel

(1) Tous les membres du personnel de l'entrepreneur qui ont accès aux données du MDN doivent :

a. détenir, à tout le moins, une habilitation de sécurité valide décernée par le PSC de SPAC, laquelle doit faire l'objet d'un suivi;

b. se voir attribuer des privilèges système selon le critère du moindre privilège; cela signifie qu'il faut appliquer l'ensemble plus restrictif de privilèges et le principe du besoin de savoir (c.-à-d. limiter l'accès aux renseignements aux personnes qui en ont besoin dans le cadre de leurs fonctions) nécessaires à l'exécution des tâches autorisées.

(2) Aucun visiteur, étranger ou membre du personnel non autorisé ne doit avoir accès aux données du MDN, au système d'information ou à la zone où l'on traite, produit ou stocke les données du MDN, à moins de détenir une cote de fiabilité valide et d'être accompagné par un employé autorisé de l'entrepreneur.

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

(4) 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 MDN.

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

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

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

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

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

(e) l'approche de détection des initiés malveillants potentiels et les contrôles mis en œuvre pour atténuer le risque d'accès aux données du gouvernement du Canada ou de dommage à la fiabilité des services infonuagiques hébergeant les données du MDN.

30. Sécurité matérielle (centre des données et installations)

(1) Le traitement, la production et le stockage des données du MDN du présent contrat ne doivent être effectués que dans des installations qui ont été autorisées par le PSC de SPAC. Toutes les données doivent être traitées, produites et stockées d'une manière sûre qui empêche la visualisation, l'accès ou la manipulation non autorisés.

(2) Conformément au *Guide pour l'établissement des zones de sécurité matérielle G1-026* de la GRC, le SI doit être installé et exploité dans une zone de travail ou une zone de travail temporaire.

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

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

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

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

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

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

(vi) l'application de mesures de protection des données du MDN à d'autres lieux de travail (p. ex., les sites de télétravail);

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

(4) L'entrepreneur doit fournir au responsable de projet du MDN un document qui décrit les mesures de sécurité matérielle de l'entrepreneur.

(5) L'entrepreneur doit aviser le responsable de projet du MDN de tout changement apporté aux mesures de sécurité matérielle qui pourrait nuire de manière importante à la sécurité matérielle.

31. Gestion des risques de la chaîne d'approvisionnement

(1) L'entrepreneur doit prendre des mesures de sécurité pour atténuer les menaces et les vulnérabilités associées à la chaîne d'approvisionnement des services de TI en vue de préserver la confiance en ce qui concerne la sécurité des sources des systèmes d'information et les composants de TI servant à offrir les services infonuagiques. En font notamment partie la 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 avoir une approche de gestion des risques de la chaîne d'approvisionnement, dont un plan de gestion des risques de la chaîne d'approvisionnement qui est conforme à l'une des pratiques exemplaires suivantes :

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

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

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

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

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

OU

(b) présenter au MDN une copie du plan de gestion des risques de la chaîne d'approvisionnement, annuellement ou sur demande du MDN.

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

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

(1) L'entrepreneur doit détenir en permanence, pendant la réalisation du contrat, de l'offre à commandes ou de l'arrangement en matière d'approvisionnement, une attestation de VOD en vigueur, ainsi qu'une cote de protection des documents approuvée au niveau PROTÉGÉ A, délivrée par la Direction de la sécurité industrielle canadienne, de **SPAC**.

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

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

(a) Liste de vérification relative à la sécurité et guide de sécurité (le cas échéant);

(b) Manuel de la sécurité industrielle (dernière édition);

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

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

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

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

(1) **L'entrepreneur ou le sous-traitant** atteste que la livraison et la prestation des services infonuagiques prévus par le présent contrat doivent provenir d'un pays membre de l'OTAN, de l'UE ou d'un pays avec lequel le Canada a conclu une entente internationale bilatérale sur la sécurité. Dans le cadre du PSC, des accords internationaux bilatéraux en matière de sécurité ont été conclus avec les pays énumérés sur le site Web https://www.tpsgc-pwgsc.gc.ca/esc-src/international-fra.html de SPAC, tel qu'il est mis à jour de temps à autre.

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

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

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

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

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

(d) Les renseignements personnels et les biens de niveau **PROTÉGÉ AU CANADA** qui sont fournis à **l'entrepreneur ou au sous-traitant** étranger destinataire, ou qui sont produits par ce dernier, doivent respecter les conditions suivantes :

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

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

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

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

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

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

National Defence | Défense nationale

National Defence Headquarters
Ottawa, Ontario
K1A 0K2

Quartier général de la Défense nationale
Ottawa (Ontario)
K1A 0K2

APPENDICE 4 DE L'ANNEXE C – DOCUMENT SUR LE POSTE DE TRAVAIL ISOLÉ

Ministère de la Défense nationale (MDN)

Document sur le poste de travail isolé

pour le

Contrat W6369-22-A009 Modification 1

1. Introduction

1.1 Le présent document décrit les exigences en matière de sécurité des TI en ce qui concerne le contrat W6369-22-A009 Modification 1 du MDN quant au transfert de renseignements électroniques entre le SI utilisé pour traiter, produire et stocker les renseignements de nature exclusive de niveau Protégé A et moins du présent contrat. La portée du présent document sur le poste de travail isolé du contrat W6369-22-A009 Modification 1 consiste à énoncer les exigences minimales en matière de sécurité des TI relativement au transfert de renseignements électroniques vers le SI et depuis celui-ci.

1.2 Dans le présent document uniquement, l'expression « renseignements exclusifs » désigne tous les biens et renseignements de nature délicate (désignés ou classifiés) du gouvernement que stocke, traite et produit un organisme privé quelconque pour exécuter un contrat conclu avec le MDN, contrat dont la sécurité est assurée par l'intermédiaire du PSC de SPAC.

1.3 Comme le contrat peut nécessiter des intrants de données de sources non fiables, il y a un besoin pour un niveau supplémentaire de sécurité des TI pour atténuer les possibilités d'infections ou de maliciels provenant de sources non fiables. Ces étapes supplémentaires visent à protéger non seulement le SI, mais aussi d'autres SI avec lesquels ce SI échangera des renseignements. Le transfert de tous les renseignements exclusifs dans le SI devra être effectué au moyen d'un ordinateur isolé.

1.4 L'application des mesures de sécurité des TI énumérées dans le présent document est fondée sur l'exigence obligatoire stipulant que les locaux doivent avoir été inspectés, évalués et autorisés pour le traitement, la production et le stockage de l'information de niveau Protégé A. Le PSC de SPAC doit fournir cette validation.

2. Exigences préalables obligatoires

2.1 Description

2.1.1 Un poste de travail autonome (c.-à-d. un ordinateur de bureau ou un ordinateur portatif) équipé d'un disque dur amovible et de deux logiciels antivirus et anti-programmes malveillants approuvés et pris en charge doit être utilisé pour tous les transferts de données électroniques vers le SI. Les données électroniques transférées dans le SI peuvent seulement provenir d'un système d'un niveau de confidentialité équivalent ou inférieur.

2.1.2 Le transfert des données électroniques dans le SI doit d'abord être autorisé par écrit par l'officier de projet du MDN.

2.2 Terminologie

2.2.1 Les termes suivants seront employés dans le présent document.

Fichier source	Données à transférer dans le système cible; le fichier source ne doit pas avoir un niveau de confidentialité supérieur au système cible.
Système source	SI d'où provient le fichier source.
Système cible	SI dans lequel le fichier source sera versé. Le système cible est le SI.
Support de transfert source	Support électronique amovible (CD, DVD, clé USB, carte SD, disque dur externe, etc.) qui contient le fichier source du système source. Dans le cas du SI, le type ou les types de supports de transfert source seront des clés USB, de même que tout autre type de support amovible approuvé par écrit par le responsable de projet du MDN.
Support de transfert cible	Support électronique amovible à utiliser pour déplacer vers le système cible le fichier source du poste de travail isolé du contrat W6369-22-A009 Modification 1. Dans le cas du SI, le type ou les types de supports de transfert cible seront des clés USB, de même que tout autre type de support amovible approuvé par écrit par le responsable de projet du MDN.

2.3 Matériel informatique

2.3.1 L'ordinateur isolé du contrat doit uniquement être utilisé aux fins précisées, et ce, pendant toute la durée du contrat.

2.3.2 Le poste de travail isolé doit être la propriété de l'entrepreneur, qui doit l'installer et le configurer pour qu'il soit complètement fonctionnel avant son inspection par le PSC du SPAC.

2.3.3 Ce poste devrait de préférence être constitué uniquement d'un ordinateur autonome, d'un moniteur, d'un clavier et d'une souris, ou encore d'un ordinateur portatif. Aucun autre équipement périphérique (imprimante, numériseur, etc.) ne peut être branché à l'ordinateur isolé.

2.3.4 Si l'entrepreneur utilise un ordinateur de bureau, l'ordinateur isolé doit être équipé d'un disque dur amovible.

2.3.5 Le poste de travail isolé doit être installé et exploité dans la même zone de travail ou dans la même zone de travail temporaire que celle où est installé le SI.

2.3.6 Étiquetage. L'ordinateur isolé du contrat et le disque dur amovible (s'il y a lieu) doivent comporter une étiquette qui identifie le niveau de confidentialité le plus élevé des renseignements exclusifs du contrat qui sont transférés au moyen de cet équipement.

2.3.7 Étiquetage du support de transfert. Le support de transfert qui sera utilisé avec l'ordinateur isolé du contrat doit comporter une étiquette avec les renseignements suivants :

2.3.7.1 le niveau de confidentialité le plus élevé des données contenues,

2.3.7.2 le ministère fédéral (dans ce cas-ci, le MDN),

2.3.7.3 le numéro de contrat (dans ce cas-ci, W6369-22-A009 Modification 1),

2.3.7.4 l'identifiant unique du support de TI, comme mentionné au paragraphe 3.5.3.2 du « Document sur les exigences relatives à la sécurité des TI du contrat W6369-22-A009 Modification 1 »,

2.3.7.5 la catégorie de support de transfert (soit « support de transfert source » ou « support de transfert cible »).

2.3.8 Si ces renseignements ne peuvent pas être inscrits directement sur le support ou si une grande étiquette (environ 4 po sur 6 po ou 10 cm sur 15 cm) ne peut pas être apposée directement sur le support, l'étiquette doit être attachée au support informatique d'une autre façon (ficelle, etc.).

2.3.9 Le support de transfert source et le support de transfert cible doivent être étiquetés avec des couleurs distinctes (p. ex., noir pour l'un et rouge pour l'autre) afin de pouvoir les différencier facilement.

Figure 1 : Exemples d'étiquettes

2.4 Configuration du système technologique

2.4.1 Le poste de travail isolé doit exécuter un système d'exploitation compatible conforme en tout point au contenu du paragraphe « Système d'exploitation » du « Document sur les exigences relatives à la sécurité des TI du contrat W6369-22-A009 Modification 1 ». Tous les processus, services et ports non essentiels doivent être désactivés, tout comme l'ensemble des composants informatiques non essentiels (carte réseau, microphone, haut-parleurs, etc.).

2.4.2 Deux logiciels antivirus et anti-programmes malveillants doivent être installés sur l'ordinateur isolé du contrat et ces logiciels doivent être pris en charge. Le poste de travail isolé du contrat doit être en tout point conforme au paragraphe « Logiciels antivirus et antimaliciels » du « Document sur les exigences relatives à la sécurité des TI du contrat W6369-22-A009 Modification 1 ».

2.4.3 Toute autre application installée sur l'ordinateur isolé du contrat devra être supprimée et désinstallée, et aucune autre application ne peut être installée sur cet ordinateur.

2.4.4 Les fonctions d'audit du système d'exploitation doivent être activées sur le poste de travail isolé du contrat, qui doit respecter en tout point le paragraphe « Ouverture de session et audit » du « Document sur les exigences relatives à la sécurité des TI du contrat W6369-22-A009 Modification 1 ».

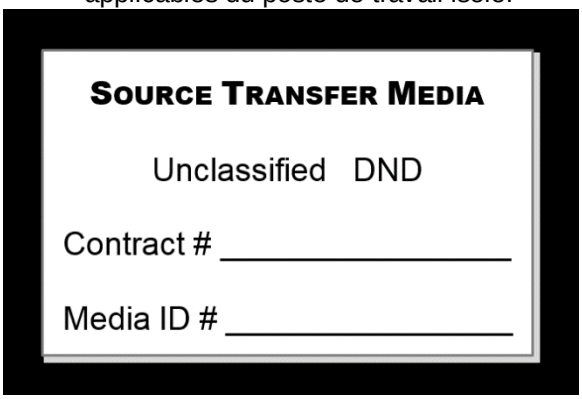
2.4.5 Tous les comptes du poste de travail isolé du contrat doivent respecter les clauses applicables du paragraphe « Autorisations et contrôle des accès » du « Document sur les exigences relatives à la sécurité des TI du contrat W6369-22-A009 Modification 1 ». Les comptes partagés ou génériques ne sont pas autorisés.

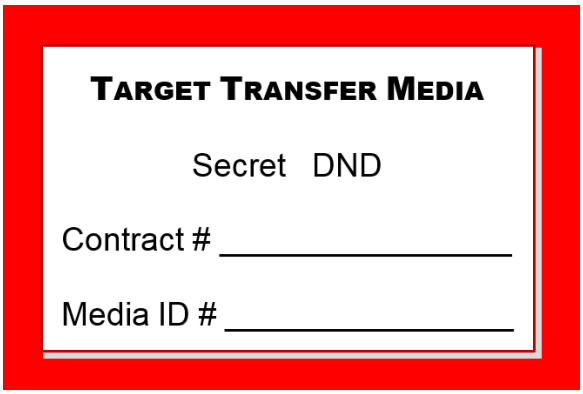
2.4.6 Les paragraphes suivants du « Document sur les exigences relatives à la sécurité des TI du contrat W6369-22-A009 Modification 1 » s'appliquent au poste de travail isolé, et doivent être respectés :

- Protection des renseignements statiques,
- Supports de TI,
- Élimination.

2.5 Ordinateur isolé et procédures opérationnelles normalisées (PON)

2.5.1 Les PON du SI doivent inclure les procédures et détails du présent « Document sur le poste de travail isolé du contrat W6369-22-A009 Modification 1 » pour tous les aspects applicables du poste de travail isolé.





3. PROCÉDURES DE TRANSFERT DE DONNÉES

3.1 Les procédures ci-dessous doivent être utilisées pour transférer des données électroniques provenant de n'importe quelle source non fiable dans le SI.

3.2 Ces procédures de transfert de données doivent être affichées à proximité du poste de travail isolé du contrat W6369-22-A009 Modification 1.

National Defence | Défense nationale

National Defence Headquarters
Ottawa, Ontario
K1A 0K2

Quartier général de la Défense nationale
Ottawa (Ontario)
K1A 0K2

PROCÉDURES DE TRANSFERT DE DONNÉES

1. Mettez le poste de travail isolé du contrat W6369-22-A009 Modification 1 sous tension et ouvrez une session.
2. Assurez-vous que les fichiers de définition des deux logiciels antivirus et antiprogrammes malveillants sont à jour. Si ce n'est pas le cas, faites les mises à jour nécessaires avant de passer à l'étape suivante.
3. Copiez les fichiers sources du système source sur le support de transfert source. Si les fichiers sources sont déjà sur un support électronique amovible (support amovible reçu d'un fournisseur, etc.), ce support peut être utilisé comme support de transfert source.
4. Étiquetez le support de transfert source et branchez-le à l'ordinateur isolé.
5. Analysez le support de transfert source et tous les fichiers sources au moyen des deux logiciels antivirus et antiprogrammes malveillants.
    a. Si un virus ou un maliciel est détecté, ARRÊTEZ la procédure. Nettoyez ou supprimez les fichiers conformément aux invites des logiciels antivirus et anti-programmes malveillants et avisez l'agent de sécurité d'entreprise ou l'agent remplaçant de sécurité d'entreprise.
    b. Si aucun virus ou maliciel n'est détecté, passez à l'étape suivante.
6. Copiez les fichiers sources du support de transfert source sur l'ordinateur isolé.
7. Débranchez le support de transfert source de l'ordinateur isolé.
8. Étiquetez le support de transfert cible et branchez-le à l'ordinateur isolé.
9. Copiez les fichiers sources analysés de l'ordinateur isolé sur le support de transfert cible.
10. Débranchez le support de transfert cible de l'ordinateur isolé.
11. Branchez le support de transfert cible au système cible.
12. Copiez les fichiers sources analysés du support de transfert cible sur le système cible.
13. Assurez-vous que les fichiers sources analysés copiés sur le système cible peuvent être ouverts et ne sont pas corrompus.
14. Si les fichiers sources sur le système cible sont satisfaisants :
    a. supprimez les fichiers sources du support de transfert cible;
    b. débranchez le support de transfert cible du système cible;
    c. supprimez les fichiers sources de l'ordinateur isolé.
15. Fermez votre session et mettez l'ordinateur isolé hors tension.