Public Works and Government Services Canada | Travaux publics et Services gouvernementaux Canada

RETURN BIDS TO:
RETOURNER LES SOUMISSIONS À:

Bid Receiving - PWGSC / Réception des soumissions - TPSGC
11 Laurier St. / 11, rue Laurier
Place du Portage , Phase III
Core 0B2 / Noyau 0B2
Gatineau
Québec
K1A 0S5
Bid Fax: (819) 997-9776

SOLICITATION AMENDMENT
MODIFICATION DE L'INVITATION

The referenced document is hereby revised; unless otherwise indicated, all other terms and conditions of the Solicitation remain the same.

Ce document est par la présente révisé; sauf indication contraire, les modalités de l'invitation demeurent les mêmes.

Comments - Commentaires

Vendor/Firm Name and Address
Raison sociale et adresse du fournisseur/de l'entrepreneur

Issuing Office - Bureau de distribution

Electronics, Simulators and Defence Systems Div.
/Division des systèmes électroniques et des systèmes de simulation et de défense
11 Laurier St. / 11, rue Laurier
8C2, Place du Portage
Gatineau
Québec
K1A 0S5

Title - Sujet Remote Minehunting and Disposal Sys Système de détection et d'élimination des mines sous-marines	
Solicitation No. - N° de l'invitation W8472-105270/C	**Amendment No. - N° modif.** 002
Client Reference No. - N° de référence du client W8472-105270	**Date** 2021-09-21
GETS Reference No. - N° de référence de SEAG PW-$$QF-125-28275	
File No. - N° de dossier 125qf.W8472-105270	**CCC No./N° CCC - FMS No./N° VME**

Solicitation Closes - L'invitation prend fin
at - à 02:00 PM Eastern Daylight Saving Time EDT
on - le 2021-11-10 Heure Avancée de l'Est HAE

F.O.B. - F.A.B. Specified Herein - Précisé dans les présentes
Plant-Usine: ☐ **Destination:** ☐ **Other-Autre:** ☑

Address Enquiries to: - Adresser toutes questions à: Lacoursiere, Paul	**Buyer Id - Id de l'acheteur** 125qf
Telephone No. - N° de téléphone (343) 551-1529 ( )	**FAX No. - N° de FAX** ( ) -

Destination - of Goods, Services, and Construction:
Destination - des biens, services et construction:

Instructions: See Herein

Instructions: Voir aux présentes

Delivery Required - Livraison exigée	**Delivery Offered - Livraison proposée**

Vendor/Firm Name and Address
Raison sociale et adresse du fournisseur/de l'entrepreneur

Telephone No. - N° de téléphone
Facsimile No. - N° de télécopieur

Name and title of person authorized to sign on behalf of Vendor/Firm (type or print)
Nom et titre de la personne autorisée à signer au nom du fournisseur/ de l'entrepreneur (taper ou écrire en caractères d'imprimerie)

Signature **Date**

Canada

Cette demande de proposition (DDP) Modification # 002 pour le système de chasse et d'élimination des mines à distance (SDEMS) vise à :

1. Fournir des réponses aux questions de l'industrie ;
2. Apportez des mises à jour à la documentation de sollicitation.

1. Veuillez consulter les questions ci-dessous avec les réponses :

Question 10,

Étant donné que la solution proposée doit être COTS et/ou MilCOTS, nous nous attendons à ce que notre fournisseur d'équipement soit considéré un fournisseur (et non un sous-traitant) de notre entreprise. Est-ce que le Canada pourrait confirmer que nous pouvons proposer un RD fourni par le fournisseur d'un soumissionnaire ?

Réponse 10,

Non. Le représentant détaché (RD) fourni pour l'évaluation devrait être la même ressource disponible pour fournir des services de RD dans le cadre du contrat du soutien en service.

Question 11,

Le volume 1, le paragraphe 3.1 précise la section IV : Renseignements complémentaires, mais le paragraphe 3.1.5 précise la section IV : Proposition de valeur. Est-ce que le Canada peut fournir une clarification ?

Réponse 11,

Oui. Le volume 1 sera modifié pour préciser la section IV : Proposition de valeur et la section V : Renseignements supplémentaires.

Question 12,

Nous demandons respectueusement au Canada d'accepter de plafonner la responsabilité de l'entrepreneur pour les dommages causés au Canada à un montant spécifique convenu mutuellement qui ne soit pas supérieur à la valeur du contrat.

Le paragraphe 7.15 du volume 2 contient un en-tête, Limitation de la responsabilité, mais sans aucun texte en dessous.

Réponse 12,

Le Canada suivra le Manuel des clauses et conditions uniformisées d'achat (CCUA) 2030 (2020-05-28), Conditions générales - Besoins plus complexes de biens, et le paragraphe 7.15 et l'en-tête sera supprimé.

Question 13,

Le Canada peut-il confirmer que le paragraphe 3.2.3.8 de l'appendice 1 de l'annexe A du volume 2 doit se lire comme suit : "Le VSA léger devrait avoir ...".

Réponse 13,

Oui. Voir l'amendement au volume 2, annexe A, appendice 1, paragraphe 3.2.3.8.

Question 14,

Les exigences en matière de chocs mécaniques conformément à la norme D-03-003-007/SG-000 Grade 1 Type A décrites dans la section 7.2 du document sur les exigences du système (Volume 2, Annexe A, Appendice 1) impliquent une qualification de chocs lourds dans une installation d'essai certifiée utilisant la plate-forme de chocs flottante. Les coûts supplémentaires et les impacts sur le calendrier doivent-ils être reflétés dans la proposition de chaque soumissionnaire ?

Réponse 14,

Oui. Il est exigé que tous les coûts et le calendrier associés aux tests environnementaux et à la qualification soient inclus dans la proposition du soumissionnaire.

Question 15,

Le Canada peut-il préciser quel niveau de contrôle de la sécurité du personnel est requis ?

Réponse 15,

Un niveau de contrôle de la sécurité du personnel SECRET est requis. Veuillez consulter les modifications apportées aux volumes 2 et 3, annexe C.

Question 16,

Le Canada pourrait-il confirmer si les informations exclusives qui ne sont pas des informations ou des données PROTÉGÉES et/ou CLASSIFIÉES sont soumises aux exigences du "Document sur les exigences de sécurité des technologies de l'information" ?

Réponse 16,

Non, ce n'est pas le cas. Seules les informations PROTÉGÉES et/ou CLASSIFIÉES sont soumises au "Document sur les exigences de sécurité de l'information".

Question 17,

Il est possible qu'un ou plusieurs des principaux sous-systèmes du SDEMS proviennent d'une ou de plusieurs entreprises qui n'ont pas de bureaux au Canada. Le Canada pourrait-il reconsidérer l'exigence 2.2.4 du "Document sur les exigences de sécurité des technologies de l'information" ?

Réponse 17,

L'exigence a été mise à jour. Veuillez voir l'amendement au volume 2 and 3, annexe C, appendice 1, "Document sur les exigences de sécurité des technologies de l'information", paragraphe 2.2.4.

Question 18,

Le Canada peut-il clarifier le terme "désigné" dans le "Document sur les exigences de sécurité des technologies de l'information" ?

Réponse 18,

"Désigné" comprend tous les niveaux de "PROTÉGÉ".

Question 19,

Nous demandons respectueusement au Canada d'accepter de plafonner la responsabilité de l'entrepreneur pour les dommages causés au Canada à un montant spécifique convenu mutuellement qui ne soit pas supérieur à la valeur du contrat. Le paragraphe 7.16 du volume 3 contient un en-tête, Limitation de la responsabilité, mais sans aucun texte en dessous.

Réponse 19,

Le Canada suivra le Manuel des clauses et conditions uniformisées d'achat (CCUA) 2035 (2018-06-21), Conditions générales – besoins plus complexes de services et le paragraphe 7.16 et l'en-tête sera supprimé.

Question 20,

L'article 11c de la partie A de la LVERS pour le soutien en service (SSS) stipule qu'aucune production (fabrication, et/ou réparation et/ou modification) de matériel ou d'équipement PROTÉGÉ et/ou CLASSIFIÉ n'aura lieu sur le site ou dans les locaux du fournisseur.

Le Canada peut-il préciser cette exigence, car on s'attend à ce que l'équipement du Système de détection et d'élimination des mines sous-marines (SDEMS) doit être réparé et/ou modifié sur le site de l'entrepreneur dans le cadre du contrat ISS?

Réponse 20,

Les soumissions peuvent inclure ou non des équipements PROTÉGÉS et/ou CLASSIFIÉS. S'il est déterminé que l'équipement ou les composants de la proposition du soumissionnaire sont de nature sensible (PROTÉGÉ et/ou CLASSIFIÉ), la LVERS et les clauses de sécurité du contrat devront être modifiées, y compris le niveau de capacité de sauvegarde des documents (DSC), et il faudra démontrer qu'elles sont respectées avant l'attribution du contrat.

2. Veuillez consulter les modifications suivantes aux documents de sollicitation.

8, Au Volume 1, paragraphe 3.1;

Supprimer : Section IV : Renseignements supplémentaires
Insérer : Section IV : Proposition de valeur
Section V : Renseignements supplémentaires

9, Au Volume 1, paragraphe 6.1(e);

Supprimer : section IV
Insérer : section V

10, Au Volume 2, paragraphe 7.15;

Supprimer : tout le paragraphe 7.15

11, Au volume 2, annexe A, appendice 1, paragraphe 3.2.3.8;

Supprimer : tout le paragraphe
Insérer : Le VSA léger devrait avoir un taux de couverture, en mode de détection seulement, d'au moins 0,40 km2/h ou plus dans un fond de type A1 tout en respectant la résolution sonar minimale

12, Au Volume 2, annexe C;

Supprimer : toute l'annexe C
Insérer : Volume 2, annexe C

ANNEXE C

Liste de vérification des exigences relative à la sécurité

Système de détection et d'élimination des mines sous-marines

Version électronique est disponible de l'autorité de contracte

Contract Number / Numéro du contrat
W8472-105270 Amendment 2

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 Organizati Ministère ou organisme gouvernemental d'origine: Department of National Defence	2. Branch or Directorate / Direction générale ou Direction DGMEPM/MSC
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 work required delivery of the Remote Minehunting and Disposal System. The effort includes delivery of all subsystems, integration into a containerized solution and delivery of integrated logistics support including technical documentation and training.

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

Canada	NATO / OTAN	Foreign / Étranger
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)

[redacted]

Contract Number / Numéro du contrat	
W8472-105270 Amendment 2	
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 :

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?

On DND premises, unscreened pers. may only access public/reception zones

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?

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	B	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).

Contract Number / Numéro du contrat
W8472-105270 Amendment 2
Security Classification / Classification de sécurité
Unclassified

PART D - AUTHORIZATION / PARTIE D - AUTORISATION

13. Organization Project Authority / Chargé de projet de l'organisme

Name (print) - Nom (en lettres moulées)	Title - Titre	Signature	
Shawn Beaudette	MSC 7-2	BEAUDETTE, SHAWN 529	Digitally signed by BEAUDETTE, SHAWN 529 Date: 2020.12.01 12:26:14 -05'00'

Telephone No. - N° de téléphone	Facsimile No. - N° de télécopieur	E-mail address - Adresse courriel	Date
613-762-7039		Shawn.Beaudette@forces.gc.ca	2021-08-17

14. Organization Security Authority / Responsable de la sécurité de l'organisme

Name (print) - Nom (en lettres moulées)	Title - Titre	Signature	
Sasa Medjovic	Senior security analyst	MEDJOVIC SASHA 234	Digitally signed by MEDJOVIC, SASHA 234 DN: C=CA, O=GC, OU=DND-MDN, OU=Personnel, OU=INTERN, CN=MEDJOVIC, SASHA 234 Reason: I am the author of this document Location: your signing location here Date: 2021.08.20 13:37:13-04'00' Foxit PhantomPDF Version: 10.1.4

Telephone No. - N° de téléphone	Facsimile No. - N° de télécopieur	E-mail address - Adresse courriel	Date
613-996-0286		sasa.medjovic@forces.gc.ca	

15. Are there additional instructions (e.g. Security Guide, Security Classification Guide) attached?
Des instructions supplémentaires (p. ex. Guide de sécurité, Guide de classification de la sécurité) sont-elles jointes?

☑ No / Non ☐ Yes / Oui

16. Procurement Officer / Agent d'approvisionnement

Name (print) - Nom (en lettres moulées)	Title - Titre	Signature
Paul Lacoursiere	Supply Team Lead; Navigation, Sonar and Radar Systrems	

Telephone No. - N° de téléphone	Facsimile No. - N° de télécopieur	E-mail address - Adresse courriel	Date
343-551-1529		Paul.Lacoursiere@	

17. Contracting Security Authority / Autorité contractante en matière de sécurité

Name (print) - Nom (en lettres moulées)	Title - Titre	Signature
C. Jason Quade Contract Security Officer Jason.Quade@pwgsc-tpsgc.gc.ca		

- N° de télécopieur	E-mail address - Adresse courriel	Date

ANNEXE C

Appendice 1

Ministère de la Défense nationale (MDN)

Document sur les exigences relatives à la sécurité des technologies de l'information

pour le

contrat W8472-105270

HISTORIQUE DES VERSIONS

VERSION	DATE DE MODIFICATION	DÉTAILS DES MODIFICATIONS	MODIFIÉ PAR
1.0	2021-03-25	Version initiale	Capt Martineau, Dir Sécur GI
1.1	2021-03-26	Version définitive	Julie Bastarache, DIM Secur
1.2	2021-08-13	Amendement 2, paragraphe 2.2.4	Shawn Beaudette, DIM Secur
1.3	2021-08-17	Accepté l'amendement proposé au paragraphe 2.2.4. Version finale	Rob Kabano, DIM Secur

TABLE DES MATIÈRES

1. INTRODUCTION

1.1 Document sur les exigences relatives à la sécurité des technologies de l'information. Le présent document, intitulé « Document sur les exigences relatives à la sécurité des technologies de l'information (TI) pour le contrat W8472-105270 » est fourni conformément aux directives pour établir la section 11.d de la partie C du formulaire 350-103 du Secrétariat du Conseil du Trésor (SCT), lesquelles stipulent que :

> […] « le fournisseur sera-t-il tenu d'utiliser ses systèmes informatiques pour traiter, produire ou stocker électroniquement des renseignements ou des données PROTÉGÉS ou CLASSIFIÉS? » Dans l'affirmative [...] le ministère ou l'organisme client doit préciser dans un document technique distinct les exigences relatives à la sécurité des TI associées à cet achat [...].

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 W8472-105270 » est spécifique au contrat W8472-105270.

1.2 Exigences du MDN en matière de sécurité des TI. Le présent document décrit les exigences du ministère de la Défense nationale (MDN) en matière de sécurité des TI servant à stocker, à traiter et à produire les renseignements exclusifs du contrat susmentionné, dont la cote de sécurité est CONFIDENTIEL et OTAN CONFIDENTIEL ou inférieure.

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. Comme le stipulent l'énoncé des travaux (EDT) et ses annexes, l'entrepreneur est limité aux seuls renseignements non classifiés dans l'environnement de données partagé (EDP). Il lui est interdit de stocker, de traiter, de produire et de transmettre des données classifiées ou des marchandises contrôlées dans cet environnement.

1.5 Couches de protection de la sécurité. La sécurité repose sur diverses couches de protection. En d'autres termes, les exigences en matière de sécurité des TI protègent efficacement l'information lorsqu'on s'y conforme, mais à condition que d'autres mesures et politiques de sécurité les sous-tendent. Il ne faut donc réaliser des travaux en sous-traitance qu'après avoir mis en œuvre des mesures pour protéger la sécurité du matériel, ainsi que celle du personnel, des procédures, de l'information 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. D'autres renseignements portant sur la sécurité sont disponibles en ligne auprès du PSC de SPAC, du Centre de la sécurité des télécommunications (CST), du Centre canadien pour la cybersécurité (CCC) et de 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 en matière de sécurité, les autres exigences énoncées dans ce document doivent être satisfaites. Si deux exigences portent sur le même enjeu, on doit appliquer la plus stricte.

2.1.2 Lieux de travail de l'entrepreneur. L'entrepreneur doit communiquer au PSC de SPAC et à l'officier de projet (OP) du MDN tous les emplacements où il a l'intention de stocker, de traiter et de produire des renseignements exclusifs CONFIDENTIEL et OTAN CONFIDENTIEL ayant trait au présent contrat. Ces emplacements comprennent les locaux de l'entrepreneur principal ou d'un autre entrepreneur, les chantiers de construction, les emplacements de stockage de secours, les locaux de partenaires, les locaux des sous-traitants de tous niveaux, etc.

2.1.3 Exigences relatives aux emplacements. Selon le cas, une attestation de sécurité d'installation (ASI), une vérification d'organisation désignée (VOD) ou une autorisation de détenir des renseignements (ADR) doit être attribuée à tout emplacement où l'entrepreneur stocke, traite ou produit des renseignements exclusifs ayant trait au présent contrat. Le PSC de SPAC doit également attester de la sécurité des différents emplacements avant que l'entrepreneur ne soit autorisé à y stocker, traiter et produire de tels renseignements exclusifs.

2.1.4 Sécurité des émissions (EMSEC). Étant donné que le présent contrat a été évalué au niveau CONFIDENTIEL et OTAN CONFIDENTIEL, l'entrepreneur doit se conformer aux spécifications de sécurité des émissions (EMSEC), telles que décrites dans le guide ITSG-11A, Conseils relatifs à la sécurité des émissions (EMSEC), du CST/CCC. Cette publication peut être obtenue auprès du PSC de SPAC ou de l'OP du MDN.

2.2 Sécurité du matériel

2.2.1 Installations autorisées. Le stockage, le traitement et la production de renseignements exclusifs ayant trait au présent contrat ne peuvent s'effectuer que dans les installations autorisées par le PSC de SPAC. Toutes les données doivent être stockées, traitées et produites en toute sécurité, de façon à empêcher quiconque de les voir, d'y accéder ou de les manipuler.

2.2.2 Zone de sécurité du matériel. Conformément au guide pour l'établissement des zones de sécurité du matériel G1-206 de la GRC, le système d'information, appelé SI W8472-105270 dans le présent document, doit être installé et exploité dans une zone de sécurité.

2.2.3 Zone de sécurité du matériel – Liste de contrôle de l'accès. Une liste de contrôle de l'accès (LCA) régit les entrées dans la zone de sécurité. Une copie papier de cette liste doit être affichée à l'intérieur de la zone où le système d'information (SI) est installé et exploité. Il incombe à l'agent de sécurité d'entreprise (ASE) ou à l'agent remplaçant de sécurité d'entreprise (ARS) de mettre à jour cette liste lorsqu'un changement survient dans la composition du personnel autorisé à accéder à la zone de sécurité.

2.2.4 Renseignements exclusifs à l'extérieur du Canada. En vertu du présent contrat, il est permit de stocker, de traiter et de produire des renseignements exclusifs à l'extérieur du Canada, sous réserve des conditions suivantes.

2.2.4.1 Conformément à la section 9.8 du MSC, lorsqu'elles attribuent des contrats, y compris des contrats de sous-traitance, à des organisations situées à l'extérieur du Canada qui détiennent une attestation de sécurité d'installation (ASI) valide dans leur pays (entrepreneur étranger), les organisations sont tenues d'obtenir l'approbation de l'AVD canadienne pour le contrat et/ou le contrat de sous-traitance.

2.2.4.2 L'entrepreneur étranger doit respecter toutes les conditions énoncées dans le " Document sur les exigences en matière de sécurité des TI pour le contrat W8472-105270 " et dans le " Document sur les ordinateurs du périmètre aérien pour le contrat W8472-105270 ".

2.2.4.3 Toute question concernant le PSPC/CSP à l'intérieur du Canada sera traitée à l'extérieur du Canada par l'autorité de sécurité désignée canadienne (ASD canadienne).

2.2.4.4 S'il n'est pas en mesure de respecter toutes les exigences en matière de sécurité, l'entrepreneur étranger est tenu de fournir des " mesures d'atténuation proposées par rapport à des exigences précises " qui seront examinées par l'OP du MDN, puis discutées avec l'entrepreneur étranger afin de déterminer les mesures de protection acceptables pour le MDN.

2.2.5 Informatique mobile et télétravail. En vertu du présent contrat, les membres du personnel à l'emploi de l'entrepreneur n'ont pas le droit d'utiliser l'informatique mobile ou de faire du télétravail depuis leur domicile lorsqu'ils stockent, traitent ou produisent des renseignements exclusifs ou qu'ils utilisent le SI d'une manière ou d'une autre.

2.3 Sécurité du personnel

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

2.3.1.1 détenir au moins une cote de sécurité SECRET valide (niveau II) que lui accorde le PSC de SPAC et qui en assure également le suivi;

2.3.1.2 se voir attribuer les privilèges d'utilisation du système selon le critère du moindre privilège. Cela signifie qu'il faut appliquer l'ensemble de privilèges le plus restrictif et le principe du besoin de savoir (à savoir, limiter l'accès à l'information aux seules personnes qui en ont besoin dans l'exercice de leurs fonctions) nécessaires à l'exécution des tâches autorisées.

2.3.2 Accès à la zone de sécurité du matériel. Aucun visiteur, étranger ou membre du personnel non autorisé ne doit avoir accès aux renseignements exclusifs, au contrat SI W8472-105270 et à la zone où l'on stocke, traite ou produit l'information exclusive, sauf s'il détient une cote de sécurité SECRET valide (niveau II) et qu'il est accompagné par un employé autorisé de l'entrepreneur. Le nom de chaque visiteur, étranger et membre du personnel non autorisé qui entre dans la zone de sécurité doit être consigné dans un registre de vérification tenu à jour.

2.3.3 Cours de sensibilisation à la sécurité des TI. Tous les membres du personnel de l'entrepreneur qui sont en contact d'une manière ou d'un autre avec des renseignements exclusifs doivent suivre une formation ou assister à des séances d'information que coordonne l'ASE ou l'ARSE. La formation doit, à tout le moins, renvoyer au manuel de la sécurité des contrats (MSC) de SPAC et à tout autre renseignement sur la sécurité dont l'OP du MDN décidera de la pertinence, ainsi qu'aux ordonnances de sécurité et aux instructions permanentes d'opérations (IPO) relatives au système pour le contrat SI W8472-105270. La formation doit également porter sur l'ingénierie sociale, ou piratage psychologique, l'utilisation des médias sociaux et la connaissance de la situation.

2.4 Sécurité des procédures

2.4.1 Ordonnances de sécurité et instructions permanentes d'opérations relatives aux TI. L'entrepreneur doit rédiger des ordres de sécurité et des OPI ayant spécifiquement trait au SI, à son exploitation et à sa maintenance pour le contrat SI W8472-105270. Ces documents doivent, à tout le moins, fournir les renseignements suivants :

2.4.1.1 rôles et responsabilités (de l'ASE, du responsable technique, du ou des administrateurs du SI, etc.);

2.4.1.2 gestion des accès à la zone de sécurité et au système d'information (SI);

2.4.1.3 utilisation acceptable du SI;

2.4.1.4 procédures de gestion des incidents;

2.4.1.5 tout autre sujet mentionné dans le présent document;

2.4.1.6 tout autre enjeu ou problème relevé par l'OP du MDN ou le bureau de gestion de projet (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 contrat SI W8472-105270, ainsi que lire et signer le formulaire de consentement de l'utilisateur, tel que rédigé et suivi par l'ASE ou l'ARSE. Tout changement apporté aux ordonnances de sécurité des TI, aux IPO et au formulaire de consentement de l'utilisateur en lien avec le SI doit être communiqué à tous les membres du personnel qui ont accès à ce système.

2.4.3 Administrateur du système – Cote de sécurité du personnel. La ou les personnes qui assurent l'administration et la maintenance du SI doivent détenir au moins une cote de sécurité SECRET valide (niveau II).

2.4.4 Surveillance constante du SI. L'entrepreneur doit surveiller en permanence sa situation générale à l'égard de la sécurité, ce qui comprend la sécurité du matériel, du personnel, des procédures, de l'information et des TI. Il doit signaler au PSC de SPAC et à l'OP du MDN tout problème susceptible de menacer la sécurité des renseignements exclusifs ou du SI.

2.5 Sécurité de l'information

2.5.1 Marquage des documents. Que ce soit dans sa version imprimée ou électronique, tout document qui contient des renseignements exclusifs doit porter la mention du niveau de sécurité le plus élevé applicable à son contenu et un identifiant unique pour en assurer adéquatement le contrôle et le suivi.

2.5.2 Information stockée. L'entrepreneur doit protéger la sécurité des renseignements exclusifs stockés en appliquant des mesures de sécurité matérielles ou informatiques.

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 (GC). Le choix du contenant dépend du niveau de confidentialité de l'information ainsi stockée. Le ou les contenants utilisés doivent satisfaire aux exigences énoncées dans le guide d'équipement de sécurité G1-001 de la GRC. Ce guide n'étant pas destiné à la population générale, l'entrepreneur doit communiquer avec l'OP du MDN pour obtenir de l'information au sujet des contenants.

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, l'information exclusive est protégée si le support est perdu, égaré ou volé.

2.5.2.3 Seuls les membres du personnel de l'entrepreneur autorisé 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 exclusifs. Les documents imprimés ou les supports informatiques amovibles utilisés pour partager des renseignements exclusifs entre le MDN et dans l'ensemble des sociétés de l'entrepreneur et de ses sous-traitants doivent être manipulés, transportés ou expédiés conformément aux lignes directrices du GC énoncées dans le MSC ou aux directives du guide G1-009 de la GRC sur le transport et la transmission de renseignements protégés ou classifiés. Qu'il soit transporté, c'est-à-dire déplacé entre deux endroits ou entre l'expéditeur et le destinataire par une personne qui a besoin de savoir et qui détient la cote de sécurité correspondant au niveau de sécurité le plus élevé des renseignements exclusifs, ou qu'il soit expédié, c'est-à-dire envoyé à un autre endroit ou à une autre personne par un tiers, le support électronique doit être chiffré avec une technologie approuvée par le GC et correspondant au niveau de confidentialité de l'information qu'il contient.

2.5.4 Échange de renseignements exclusifs – Conditionnement. Les documents imprimés et les supports informatiques doivent être conditionnés adéquatement et transportés ou expédiés avec une lettre de présentation ainsi qu'un formulaire d'envoi ou un bordereau de circulation qui indiquent :

2.5.4.1 le niveau de confidentialité le plus élevé de l'information transportée ou expédiée;

2.5.4.2 la date du transport ou de l'expédition;

2.5.4.3 l'identifiant unique de chaque document ou support informatique transporté ou expédié;

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 municipale de 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 Mise à l'écart des renseignements exclusifs à détruire d'urgence. Tous les renseignements exclusifs (sous forme de documents imprimés, de supports informatiques, etc.) doivent à l'écart des autres renseignements contractuels et ministériels de façon que l'on puisse les détruire en toute sécurité. Dès que le PSC de SPAC ou l'OP du MDN en fait la demande, comme le précise la publication ITSP.40.006 sur le nettoyage des supports informatiques du Centre canadien pour la cybersécurité (CCC).

2.5.6 Marchandises contrôlées. Pour les besoins du présent contrat, l'entrepreneur doit avoir accès à de l'information ou à du matériel dont la cote de sécurité est CONFIDENTEL, OTAN CONFIDENTIEL et désigné marchandises contrôlées.

2.5.6.1 Toutes les données désignées marchandises contrôlées du GC (sur support papier ou électronique) doivent être marquées conformément aux Directives et ordonnances administratives de la Défense DOAD 3003-1. L'entrepreneur doit se conformer à l'ensemble des règlements sur les marchandises contrôlées du GC, y compris sur l'accès et le transfert de la technologie contrôlée (ATTC) et sur le commerce international des armes (règlement ITAR des États-Unis), s'il y a lieu. Au besoin, il peut obtenir d'autres renseignements en consultant en ligne le règlement DORD/2001-32 sur les marchandises contrôlées à l'adresse https://laws-lois.justice.gc.ca/eng/regulations/SOR-2001-32/, en s'adressant au Bureau de l'ATTC par l'intermédiaire de l'OP du MDN ou en envoyant un courriel à un responsable du Programme des marchandises contrôlées (PMC) à l'adresse dmc-cgd@tpsgc-pwgsc.gc.ca.

2.5.6.2 Si un règlement quelconque sur les marchandises contrôlées contredit l'une ou l'autre des exigences en matière de sécurité des TI énoncées dans les présentes, le règlement le plus rigoureux ou l'exigence la plus rigoureuse doit s'appliquer.

2.5.7 Sous-traitants. L'entrepreneur doit signaler à l'OP du MDN et inscrire auprès du PSC de SPAC tout partenaire et sous-traitant qui prend part à l'exécution du présent contrat. C'est à l'entrepreneur qu'incombe la responsabilité de communiquer à ses sociétés et à ses sous-traitants toutes les exigences relatives à la sécurité et de leur fournir tous les documents sur la sécurité, pertinents ou afférents au présent contrat.

2.5.8 Exigences en matière de sécurité des TI pour les contrats en sous-traitance. Toutes les exigences relatives à la sécurité des TI pour le présent contrat s'appliquent également à n'importe quel contrat donné en sous-traitance.

3. EXIGENCES MINIMALES RELATIVES À LA SÉCURITÉ DES TI

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

À la fréquence et selon le calendrier qu'établira le responsable de la sécurité des TI du MDN, le Ministère se réserve le droit d'inspecter les différentes installations de chaque entrepreneur participant au présent contrat afin d'assurer leur conformité aux exigences relatives à la sécurité des TI énoncées dans les présentes, ainsi qu'aux normes et politiques du GC en matière de prévention, de détection, d'intervention et de récupération.

3.2 Configuration du système informatique

3.2.1 Type de système. Le système d'information doit être autonome, c'est-à-dire ne dépendre d'aucun autre.

3.2.2 Type de matériel. Le matériel informatique servant à stocker, à traiter et à produire des renseignements exclusifs doit être disponible sur le marché s'il se trouve dans une zone de sécurité des messages MSEC certifiée, sinon l'entrepreneur doit utiliser du matériel TEMPEST. Quel que soit le type utilisé, le matériel doit être identifié avec le niveau de confidentialité le plus élevé des renseignements exclusifs qu'il sert à stocker, à traiter et à produire.

3.2.3 Disques durs du SI. Le matériel de traitement du SI doit être doté de disques durs amovibles. Par matériel de traitement du SI, on entend les postes de travail (ordinateurs de bureau, bloc-notes et tablettes électroniques), les serveurs, les dispositifs de stockage informatiques (stockage en réseau NAS et réseau de stockage SAN), les imprimantes, les scanneurs, etc.

3.2.4 Système d'exploitation. Le SI doit être doté d'un système d'exploitation (SE) compatible, c'est-à-dire que le fournisseur du SE doit créer les correctifs de sécurité et fournir leur version la plus récente. Ces correctifs doivent être installés périodiquement, au moins chaque mois. Le SE doit être configuré pour désactiver les processus, services et ports inutiles. Les IPO relatives au SI doivent indiquer la configuration du SE, ainsi que la fréquence à laquelle les correctifs de sécurité sont appliqués au SE et la méthode utilisée pour ce faire.

3.2.5 Logiciels antivirus et antimaliciels. Une application antivirus et antimaliciels compatible et fonctionnelle doit être installée sur chacun des postes de travail et des serveurs (s'il y a lieu). La version la plus récente des fichiers de définition de l'application antivirus et antimaliciels doit être installée périodiquement. Les IPO relatives au SI doivent décrire en détail la configuration de l'application antivirus et antimaliciels et préciser également la fréquence à laquelle les fichiers de définition sont mis à jour, ainsi que la méthode employée pour les installer. L'application antivirus et antimaliciels doit être configurée de telle sorte :

3.2.5.1 qu'elle permet aux seuls administrateurs du système d'apporter des modifications;

3.2.5.2 qu'elle analyse automatiquement tous les postes de travail et tous les serveurs du SI W8472-105270 à leur mise sous tension ou à des intervalles de temps préétablis, soit au moins une fois par semaine;

3.2.5.3 qu'elle analyse tout nouveau fichier introduit dans les postes de travail et les serveurs du SI à la recherche de code malveillant.

3.2.6 Logiciels et applications. Seules les applications requises aux fins du présent contrat doivent être installées sur le SI. Les correctifs à jour de ces applications doivent être installés et gérés au moyen d'un processus de gestion de la configuration défini. Les IPO relatives au SI doivent répertorier les applications installées, indiquer leur version et préciser le processus de gestion des correctifs employé avec chacune d'elles.

3.2.7 Journalisation et vérification. La journalisation du SE doit être active, et les fichiers journaux doivent être examinés au moins une fois par mois par les différents administrateurs du SI W8472-105270. 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 et sur ses comportements inhabituels, sur les perturbations imprévues des systèmes ou des services, sur les erreurs du système, etc. Seuls les administrateurs du système sont autorisés à modifier ou à supprimer les fichiers journaux, mais seulement si l'ASE ou l'ARSE les a autorisés à procéder. Les IPO relatives au SI doivent indiquer la fréquence à laquelle les fichiers journaux du SE sont examinés et la méthode employée pour ce faire.

3.3 Matériel informatique

3.3.1 Liste des équipements. L'entrepreneur doit tenir à jour une liste des équipements qui composent le SI. Elle doit au moins en préciser la marque, le modèle et la quantité et en fournir la description. Il doit remettre cette liste au PSC de SPAC et à l'OP du MDN qui en font la demande.

3.3.2 Modifications apportées au matériel informatique. L'entrepreneur doit informer le PSC de SPAC et l'OP du MDN de tout changement important apporté au matériel informatique du SI W8472-105270.

3.3.3 Technologie Bluetooth. Il est formellement interdit à l'entrepreneur d'intégrer la technologie Bluetooth au matériel informatique du système, tout comme utiliser cette technologie dans la zone de sécurité où le SI est installé, que ce soit en permanence ou temporairement. La seule exception à cette interdiction concerne les appareils médicaux, s'ils ont été approuvés. L'ASE doit être tenu informé de la présence de tout appareil médical Bluetooth utilisé à proximité du SI W8472-105270.

3.3.4 Sans-fil ou Wi-Fi. Il est formellement interdit à l'entrepreneur d'intégrer des capacités de communication sans fil ou Wi-Fi au SI.

3.3.5 Infonuagique. Il est formellement interdit à l'entrepreneur de recourir au service infonuagique d'un fournisseur pour stocker, traiter et produire des renseignements exclusifs.

3.3.6 Diagramme topologique. L'entrepreneur doit fournir sur demande un diagramme de la topologie du SI W8472-105270 au PSC de SPAC ou à l'OP du MDN. Le diagramme doit montrer la conception globale du système et y intégrer tout lien informatique vers d'autres entités ou toute connexion vers d'autres réseaux ou systèmes, s'ils existent.

3.3.7 Entretien et élimination du matériel informatique. L'entrepreneur doit suivre les directives fournies plus loin dans la section du présent document sur l'élimination du matériel informatique utilisé pour stocker, traiter et produire des renseignements exclusifs (soit les postes de travail, les serveurs, les imprimantes, les traceurs, les scanneurs, les photocopieurs et les appareils ou imprimantes multifonctions, etc.).

3.4 Autorisations et contrôle des accès

3.4.1 Liste des membres du personnel autorisé. L'entrepreneur doit tenir à jour la liste des personnes autorisées à accéder au SI. Il doit actualiser son contenu chaque fois qu'un changement d'effectif survient ou que changent les renseignements au sujet de l'une de ces personnes. La liste doit au moins contenir les renseignements suivants :

3.4.1.1 le nom des personnes;

3.4.1.2 leur cote de sécurité;

3.4.1.3 la date à laquelle leur cote de sécurité est échue;

3.4.1.4 le type d'accès qui leur est accordé (utilisateur, super-utilisateur, administrateur, etc.).

3.4.2 Comptes d'utilisateur

3.4.2.1 L'entrepreneur doit créer un compte d'administrateur pour chacun des administrateurs du système. Toute personne qui doit accéder au SI à la fois à titre d'administrateur et d'utilisateur ordinaire doit détenir deux comptes distincts créés dans le SI. Les comptes d'administrateur ne doivent jamais servir aux opérations quotidiennes courantes ou pour résoudre des problèmes autres qu'administratifs.

3.4.2.2 L'entrepreneur doit créer un compte pour chacun des utilisateurs et lui donner un nom ou identifiant unique. Aucun autre détenteur d'un compte ne peut utiliser ce nom ou identifiant pendant la durée de vie du système. L'entrepreneur doit configurer les comptes d'utilisateur en fonction des privilèges et de l'accès aux dossiers et fichiers dont leur détenteur a besoin pour accomplir ses tâches particulières.

3.4.2.3 Le SI ne doit contenir aucun des types de comptes suivants :

3.4.2.3.1 comptes génériques;

3.4.2.3.2 comptes d'invité;

3.4.2.3.3 comptes temporaires;

3.4.2.3.4 comptes partagés d'une façon ou d'une autre.

3.4.3 Mots de passe

3.4.3.1 Chaque compte doit être protégé par un mot de passe présentant une complexité minimale qui se décline comme suit :

3.4.3.1.1 au moins huit (8) caractères;

3.4.3.1.2 trois critères parmi les suivants :

- 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 (!, $, #, %, etc.);

3.4.3.1.3 restrictions de la durée de validité du mot de passe : au moins un (1) jour et au plus 90 jours;

3.4.3.1.4 interdiction de réutiliser l'un ou l'autre des dix (1) derniers mots de passe;

3.4.3.1.5 verrouillage du compte après quatre (4) tentatives de connexion infructueuses.

3.4.3.2 Le mot de passe utilisé pour accéder au SI doit :

3.4.3.2.1 être changé à la première ouverture de session;

3.4.3.2.2 être changé dès que l'on soupçonne qu'il a été compromis;

3.4.3.2.3 être différent des autres mots de passe de l'utilisateur pour accéder aux autres SI W8472-105270;

3.4.3.2.4 ne pas être enregistré par le SE ou par toute application à laquelle le SE accède;

3.4.3.2.5 ne jamais être partagé avec qui que ce soit.

3.4.3.3 Le mot de passe original de l'administrateur local pour accéder à un équipement informatique quelconque du SI doit être changé. Il est interdit d'utiliser les mots de passe par défaut du fournisseur de cet équipement. Lorsque le mot de passe de l'administrateur local est changé, il doit être consigné sur papier et placé dans une enveloppe scellée portant sur son rabat la signature de l'ASE, de l'ARSE 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 confidentialité des données traitées par le système.

3.4.4 Liste de contrôle des accès au SI. Tous les composants réseau (matériels ou virtuels) du SI doivent être surveillés et accessibles aux seuls membres du personnel autorisé (au moyen d'une liste de contrôle des accès [LCA], d'Active Directory, etc.).

3.4.5 Autorisations et contrôle des accès dans les IPO. Les IPO relatives au SI doivent inclure la description d'un processus d'autorisation et de contrôle des accès pour ajouter, désactiver et supprimer des comptes d'utilisateur.

3.5 Supports informatiques

3.5.1 Élimination des supports informatiques. Pour la durée du présent contrat, il faut éliminer tous les supports informatiques servant à stocker, à traiter et à produire des renseignements exclusifs, conformément aux directives fournies plus loin à la section sur l'élimination.

3.5.2 Retrait des supports informatiques. Lorsque du matériel informatique requiert un entretien, un dépannage ou un remplacement, **aucun support informatique contenant des renseignements exclusifs de quelque nature que ce soit** (disque dur, clé USB, disque optique, etc.) ne doit être remis à un fournisseur externe, à un fournisseur de services ou à un membre du personnel non autorisé ou mis à sa disponibilité.

3.5.3 Identification des supports informatiques. Tous les supports informatiques (disques durs internes, externes ou amovibles, disques optiques – CD et DVD – clés USB, etc.) servant à stocker, à traiter et à produire des renseignements exclusifs doivent :

3.5.3.1 servir uniquement aux fins du présent contrat;

3.5.3.2 recevoir un identifiant unique pour en assurer adéquatement le contrôle et le suivi;

3.5.3.3 être identifiés et répertoriés avec les renseignements suivants :

3.5.3.3.1 le type de support (disque optique, clé USB, etc.);

3.5.3.3.2 le niveau de confidentialité de l'information qu'ils contiennent;

3.5.3.3.3 toute restriction relative à la divulgation du contenu (s'il y a lieu);

3.5.3.3.4 le modèle et le numéro de série (s'ils existent);

3.5.3.3.5 l'identifiant unique du support informatique;

3.5.3.4 porter une étiquette pour indiquer :

3.5.3.4.1 le niveau de confidentialité le plus élevé des données qu'ils contiennent;

3.5.3.4.2 le nom du ministère (MDN dans le cas présent);

3.5.3.4.3 le numéro de contrat;

3.5.3.4.4 l'identifiant unique du support informatique.

3.5.3.5 S'il est impossible d'apposer une étiquette directement sur le support informatique, il faut trouver un autre moyen d'y parvenir (p. ex., avec une ficelle).

3.5.4 Protection des supports informatiques. Tous les supports informatiques doivent être protégés en fonction du niveau de confidentialité le plus élevé des données qu'ils contiennent. Lorsqu'on ne les utilise pas, les supports informatiques amovibles, y compris ceux qui sont défectueux, qui ont une durée de vie utile ou qu'on utilise à long terme (p. ex., pour les sauvegardes), doivent être rangés dans un contenant verrouillé et approuvé en fonction du niveau de confidentialité de leur contenu.

3.5.5 Ordinateur isolé du contrat. Dans l'éventualité où le SI doit interagir avec une source de données non fiable (Internet, un autre réseau, des supports informatiques d'une autre provenance, etc.), l'entrepreneur doit fournir un ordinateur autonome et isolé du contrat. L'OP du MDN doit fournir à l'entrepreneur un document technique distinct dans lequel sont établies les exigences relatives à la sécurité des transferts de données et les directives connexes se rapportant à l'ordinateur isolé. Le Dir Sécur Gi peut fournir sur demande un modèle de ce document technique.

3.5.6 Consignation des supports informatiques amovibles. L'emplacement de tous les supports informatiques amovibles doit être suivi et contrôlé au moyen d'un registre. Celui-ci doit contenir au moins les renseignements suivants :

3.5.6.1 le type de support (disque optique, clé USB, disque dur amovible, bande magnétique de sauvegarde, etc.);

3.5.6.2 l'identifiant unique du support informatique;

3.5.6.3 la date et l'heure auxquelles le support a été retiré;

3.5.6.4 le nom ou les initiales et la signature de la personne qui a emprunté le support;

3.5.6.5 la date et l'heure auxquelles le support a été rendu;

3.5.6.6 t le nom ou les initiales et la signature de la personne qui a rendu le support.

3.6 Dispositifs informatiques personnels (DIP)

3.6.1 L'entrepreneur doit veiller à ce que tous les dispositifs informatiques personnels (téléphones cellulaires, montres intelligentes, appareils FitBits, etc.) ne pénètrent pas dans la zone de sécurité où se trouve le SI W8472-105270.

3.7 Impression et reproduction de documents

3.7.1 Autorisation d'imprimer ou de reproduire. L'entrepreneur :

3.7.1.1 est autorisé à imprimer ou à reproduire des renseignements exclusifs dans ses locaux au moyen d'un appareil d'impression présent sur place et branché au SI au moyen d'un câble TEMPEST ou à fibre optique;

3.7.1.2 n'est pas autorisé à recourir aux services d'un tiers pour imprimer ou reproduire des renseignements exclusifs sans avoir obtenu au préalable l'approbation et l'autorisation du PSC de SPAC et de l'OP du MDN.

3.7.2 Disques durs des dispositifs d'impression ou de reproduction. Les appareils servant à reproduire des renseignements exclusifs (imprimantes, traceurs, scanneurs, photocopieurs, appareils ou imprimantes multifonctions, etc.) doivent être dotés de disques durs amovibles. L'entrepreneur doit substituer à un appareil qui n'est pas compatible avec la technologie des disques durs amovibles, un appareil d'un autre type sans disque dur interne ou doté d'un disque dur amovible.

3.7.3 Connexion d'imprimantes. À moins que le SI ne soit configuré comme un segment du réseau d'entreprise de l'entrepreneur, l'entrepreneur ne peut brancher les imprimantes, traceurs, scanneurs, photocopieurs et les appareils et imprimantes multifonctions qu'à ce système. Il lui est formellement interdit d'y brancher d'autres appareils ou réseaux.

3.7.4 Branchement de lignes téléphoniques. Il est formellement interdit à l'entrepreneur de brancher un nombre quelconque de lignes téléphoniques à un appareil ou une imprimante multifonctions servant à traiter des renseignements exclusifs.

3.7.5 Reproduction de renseignements exclusifs de nature particulièrement délicate. Quels que soient les renseignements exclusifs de nature particulièrement délicate que contient un document, son impression ou sa reproduction doit être approuvée au préalable par l'OP du MDN et chaque exemplaire du document doit recevoir un identifiant unique pour en assurer adéquatement le suivi et le contrôle.

3.8 Récupération

3.8.1 Sauvegarde du SI. L'entrepreneur doit sauvegarder périodiquement, soit au moins une fois par semaine, les renseignements exclusifs. Il doit ranger les copies de sécurité ainsi créées dans un autre endroit (p. ex., dans un autre édifice) afin d'en assurer la protection. Si l'entrepreneur n'a pas accès à un autre endroit pour ce faire, il peut prendre les dispositions nécessaires avec l'OP du MDN. Si les copies de sécurité doivent être confiées à la protection d'un organisme tiers, une telle modalité doit faire l'objet d'un contrat donné en sous-traitance. Les IPO relatives au SI doivent fournir tous les renseignements nécessaires ayant trait à la fréquence des sauvegardes, à la méthode employée et aux modalités du stockage.

3.8.2 Vérification des copies de sécurité. L'entrepreneur doit vérifier périodiquement les copies de sécurité. 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.

3.8.3 Plan de reprise après sinistre. L'entrepreneur doit concevoir et documenter un plan de reprise après sinistre (PRS) destiné au SI. Le plan doit fournir tous les renseignements nécessaires ayant trait à la récupération, à la restauration, à la fréquence des vérifications et à la méthode employée.

3.9 Élimination

3.9.1 Autorisation d'éliminer. L'OP du MDN doit autoriser au préalable l'élimination de tous les supports informatiques utilisés dans le cadre du présent contrat, y compris les supports amovibles et les disques durs internes et externes. Les activités d'élimination doivent être documentées et suivies. Plusieurs causes forcent l'élimination d'un support informatique, soit parce qu'il est défectueux, que sa durée de vie utile est terminée, qu'il ne sert plus, etc. S'il est impossible de retirer le ou les disques durs d'un appareil servant à stocker, à traiter et à produire de renseignements exclusifs (comme c'est le cas avec les tablettes électroniques, par exemple), l'entrepreneur doit rendre cet appareil à l'OP du MDN.

3.9.2 Élimination sur place. Il est formellement interdit à l'entrepreneur d'éliminer dans ses locaux tout support informatique ayant servi à stocker, à traiter et à produire de renseignements exclusifs.

3.9.3 Élimination des supports informatiques – Suivi. L'entrepreneur doit assurer le suivi de l'élimination des supports informatiques en remplissant un certificat de destruction (s'il y a lieu) et un formulaire de transmission et de réception des documents. Il peut obtenir les modèles de ces documents auprès de l'OP du MDN. 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. Il doit fournir ces documents au PSC de SPAC et à l'OP du MDN qui en font la demande.

3.9.4 Retour de tous les renseignements exclusifs. À la fin du contrat, l'entrepreneur doit retourner tous les renseignements exclusifs (copies papier et électroniques) à l'OP du MDN. Cela comprend tous les exemplaires imprimés des documents, ainsi que tous les supports informatiques ayant servi à stocker, à traiter et à produire des renseignements exclusifs (disques durs internes des postes de travail, des blocs-notes, des serveurs, des photocopieurs, des appareils et imprimantes multifonctions, etc.), les disques optiques au format CD ou DVD, les clés, les cartes mémoire SD, les disques durs externes, etc.). S'il est impossible de retirer le ou les disques durs d'un appareil servant à stocker, à traiter et à produire de renseignements exclusifs (comme c'est le cas avec les tablettes électroniques, par exemple), l'entrepreneur doit le rendre à l'OP du MDN. Si l'entrepreneur a utilisé des biens contrôlés, il doit les démilitariser de concert avec l'OP du MDN.

3.9.5 Procédures précédant le retrait du matériel informatique. L'entrepreneur doit suivre les procédures ci-dessous avant de procéder à la maintenance ou à l'élimination d'un équipement informatique servant à stocker, à traiter et à produire des renseignements exclusifs (serveur, poste de travail, imprimante, traceur, scanneur, appareil ou imprimante multifonctions, etc.).

3.9.5.1 Avec tout appareil utilisé pour imprimer des renseignements exclusifs Protégé B ou classifiés dans le cadre du présent contrat :

3.9.5.1.1 l'entrepreneur doit imprimer au moins 50 copies d'une page de texte entièrement non classifié pour éliminer toutes données susceptibles de rester présentes sur le tambour, les courroies ou tout autre composant interne de l'appareil d'impression;

3.9.5.1.2 l'entrepreneur doit éliminer toutes les cartouches de poudre d'imprimante laser comme il le fait avec les supports informatiques défectueux, dont la durée de vie utile est terminée ou qui ne servent plus. Une telle élimination a pour but d'empêcher tout incident lié aux cartouches dotées d'un tambour d'impression intégré sur lequel l'image d'un document imprimé pourrait persister.

3.9.5.2 L'entrepreneur doit retirer et éliminer tous les dispositifs de mémoire non volatile (disques durs internes, amovibles et externes, etc.) de la manière décrite dans la présente section.

3.9.5.3 L'entrepreneur doit effacer le contenu des dispositifs de mémoire volatile (barrettes de mémoire vive ordinaire [RAM], statique [SRAM] ou dynamique [DRAM], etc.) en coupant toutes leurs sources d'alimentation électrique pendant au moins 24 heures consécutives. Il doit s'assurer que la mémoire ne reçoit aucune forme d'alimentation électrique (par exemple, d'une pile interne ou par l'intermédiaire d'une connexion à un appareil). S'il subsiste un doute quant à la présence d'une source d'électricité alimentant la mémoire volatile d'un équipement servant à stocker, à traiter et à produire des renseignements exclusifs de nature très délicate, l'entrepreneur doit retirer cette mémoire et la faire détruire.

3.9.5.4 L’entrepreneur doit retirer les autocollants et effacer les marques de sécurité ayant trait au présent contrat ou au SI qui se trouvent sur l’appareil.

ANNEXE C

Appendice 2

Ministère de la Défense nationale (MDN)

Document sur le poste de travail isolé

pour le

contrat W8472-105270

HISTORIQUE DES VERSIONS

VERSION	DATE DE MODIFICATION	DÉTAILS DES MODIFICATIONS	MODIFIÉ PAR
1.0	25 mars 2021	Version initiale	Capt Martineau, Dir Sécur GI

Table des matières

1. INTRODUCTION

1.1 Le présent document décrit les exigences en matière de sécurité des technologies de l'information (TI) du ministère de la Défense nationale (MDN) pour le contrat W8472-105270 visant le transfert de données électroniques entre le système d'information (SI) nommé aux fins des présentes le SI W8472-105270; il est destiné à produire, à stocker et à traiter les renseignements exclusifs de ce contrat, jusqu'aux niveaux de confidentialité CONFIDENTIEL ou OTAN CONFIDENTIEL. Le présent « Document sur le poste de travail isolé pour le contrat W8472-105270 » vise à énoncer les exigences minimales en matière de sécurité des TI nécessaires à l'échange de données électroniques entre le SI et d'autres systèmes.

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 ministère de la Défense nationale (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).

1.3 Comme ce contrat pourrait exiger la saisie de données dont la source n'a pas été approuvée, un niveau de sécurité des TI supplémentaire est nécessaire afin de réduire la possibilité d'infection ou de maliciel provenant d'une source non approuvée. Ces étapes supplémentaires visent à protéger non seulement le SI W8472-105270, mais aussi d'autres SI avec lesquels ce SI échangera des renseignements. Le transfert de tous les renseignements contractuels dans le SI devra s'effectuer depuis un poste de travail isolé.

1.4 L'application des mesures de sécurité des TI énoncées dans le présent document est fondée sur l'exigence obligatoire selon laquelle il faut inspecter, évaluer et autoriser les lieux destinés au traitement, à la production ou au stockage de renseignements de niveau de confidentialité CONFIDENTIEL ou OTAN CONFIDENTIEL. SPAC ou le PSC doivent fournir cette validation.

2. EXIGENCES PRÉALABLES OBLIGATOIRES

2.1 Description

2.1.1 Un poste de travail autonome équipé d'un disque dur amovible et de deux logiciels antivirus/antimaliciels approuvés et compatibles doit être utilisé pour effectuer tous les transferts de données vers le SI. Les données électroniques transférées dans le SI ne peuvent provenir que d'un SI d'un niveau de confidentialité équivalent ou inférieur.

2.1.2 Le transfert des données électroniques dans le SI W8472-105270 doit être autorisé par écrit par le officier de projet (OP) du MDN.

2.2 Glossaire

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 W8472-105270.
Support de transfert source	Support électronique amovible (disque optique au format CD ou DVD, clé USB, carte SD, disque dur externe, etc.) qui contient le fichier source du système source. Pour le SI W8472-105270, le seul type de support source autorisé pour le transfert est le DVD-ROM.
Support de transfert cible	Support électronique amovible à utiliser pour déplacer le fichier source du poste de travail isolé W8472-105270 vers le système cible. Pour le SI W8472-105270, le seul type de support source autorisé pour le transfert est le DVD-ROM.

2.3 Matériel

2.3.1 Le poste de travail isolé doit se trouver dans la même zone de sécurité du matériel que le SI W8472-105270 et utiliser le même type d'équipement (commercial ou TEMPEST, par exemple), tel qu'énoncé à la section « Type d'équipement » du « Document sur les exigences relatives à la sécurité des technologies de l'information (TI) pour le contrat W8472-105270 ».

2.3.2 Le poste de travail isolé ne devra servir qu'à cela pendant toute la durée du contrat.

2.3.3 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 SPAC ou le PSC.

2.3.4 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 périphérique (imprimante, numériseur, etc.) ne peut être branché au poste de travail isolé.

2.3.5 Si ce n'est pas un ordinateur portatif, le poste de travail isolé doit être muni d'un disque dur amovible.

2.3.6 Le poste de travail isolé doit être installé et doit fonctionner dans la même zone de sécurité où est installé le SI W8472-105270.

2.3.7 Étiquetage. Le poste de travail isolé et le cas échéant le disque dur amovible doivent comporter une étiquette qui indique le niveau de confidentialité le plus élevé des renseignements exclusifs qui sont transférés à l'aide de cet équipement.

2.3.8 Étiquetage du support de transfert. Le support de transfert utilisé dans le poste de travail isolé doit comporter une étiquette indiquant les renseignements suivants :

2.3.8.1 le niveau le plus élevé de confidentialité des données contenues;

2.3.8.2 le ministère fédéral (dans ce cas, le MDN);

2.3.8.3 le numéro du contrat (ici, W8472-105270);

2.3.8.4 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 W8472-105270 »;

2.3.8.5 le type de support de transfert (« Support de transfert source » ou « Support de transfert cible »);

2.3.9 si ces renseignements ne peuvent pas être inscrits directement sur le support ou si une grande étiquette (4 po sur 6 po environ) ne peut pas être apposée directement sur le support, l'étiquette doit y être attachée d'une autre façon (ficelle, etc.);

2.3.10 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 de TI

2.4.1 Le poste de travail isolé doit exécuter un système d'exploitation (SE) 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 W8472-105270 ». 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/antimaliciels doivent être installés sur le poste de travail isolé de ce contrat, et ces logiciels doivent être compatibles. Le poste de travail isolé du contrat doit être en tout point conforme au paragraphe « Logiciels antivirus/antimaliciels » du « Document sur les exigences relatives à la sécurité des TI du contrat W8472-105270 ».

2.4.3 Toute autre application du poste de travail isolé du contrat doit être supprimée ou désinstallée, et aucune autre application ne peut être installée sur cet ordinateur.

2.4.4 Les fonctions d'audit du SE 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 W8472-105270 ».

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 W8472-105270 ». Les comptes partagés ou génériques sont interdits.

2.4.6 Les paragraphes suivants du « Document sur les exigences relatives à la sécurité des TI du contrat W8472-105270 » s'appliquent au poste de travail isolé, et doivent être respectés :

- Support amovible laissé sans surveillance;
- Supports de TI;
- Dispositifs informatiques personnels (DIP);
- Élimination.

2.5 PON visant le poste de travail isolé

2.5.1 Les PON du SI W8472-105270 doivent inclure les procédures et détails du présent « Document sur le poste de travail isolé, contrat W8472-105270 » pour tous les aspects applicables du poste de travail isolé.

3. PROCÉDURE DE TRANSFERT DES DONNÉES

3.1 La procédure ci-dessous doit être utilisée pour transférer des données électroniques provenant de toute source non fiable au SI.

3.2 Cette procédure de transfert des données doit être affichée près du poste de travail isolé W8472-105270.

PROCÉDURE DE TRANSFERT DES DONNÉES

1. Mettre le poste de travail isolé sous tension W8472-105270 et ouvrir une session.
2. S'assurer que les fichiers de définition des deux logiciels antivirus/antimaliciels sont à jour. Le cas échéant, faire les mises à jour nécessaires avant de passer à l'étape suivante.
3. Copier 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.), alors ce support devient le support de transfert source.
4. Étiqueter le support de transfert source et le brancher au poste de travail isolé.
5. Analyser le support de transfert source et tous les fichiers sources au moyen des deux logiciels antivirus/antimaliciels.
    a. Si un virus ou un maliciel est détecté, ARRÊTER la procédure. Nettoyer ou supprimer les fichiers conformément aux invites des logiciels antivirus/antimaliciels et informer l'agent de sécurité d'entreprise (ASE) ou l'agent remplaçant de sécurité d'entreprise (ARSE).
    b. Si aucun virus/maliciel n'est détecté, passer à l'étape suivante.
6. Copier les fichiers sources du support de transfert source sur le poste de travail isolé.
7. Débrancher le support de transfert source du poste de travail isolé.
8. Étiqueter le support de transfert source et le brancher au poste de travail isolé.
9. Copier sur le support de transfert cible les fichiers sources analysés du poste de travail isolé.
10. Débrancher le support de transfert cible du poste de travail isolé.
11. Brancher le support de transfert cible au système cible.
12. Copier les fichiers sources du support de transfert cible au système cible.
13. Confirmer 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. supprimer les fichiers sources du support de transfert cible;
    b. débrancher le support de transfert cible du système cible;
    c. supprimer les fichiers sources du poste de travail isolé.
15. Fermer la session et mettre le poste de travail isolé hors tension.

13, Au Volume 3, paragraphe 7.16;

Supprimer : tout le paragraphe 7.16

14, Au Volume 3, annexe C;

Supprimer : toute l'annexe C
Insérer : Volume 3, annexe C

ANNEXE C

Liste de vérification des exigences relative à la sécurité

Système de détection et d'élimination des mines sous-marines

(Version électronique est disponible de l'autorité de contracte)

Contract Number / Numéro du contrat	
W8482-206387 Amendment 2	
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 Organizati Ministère ou organisme gouvernemental d'origine	Department of National Defence	2. Branch or Directorate / Direction générale ou Direction ADM (Mat) / DGMEPM / MSC
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 work requires the provide the in-service support to the Remote Minehunting and Disposal System (RMDS). This effort includes repair and maintenance of the RMDS at the contractor facility and DND sites, engineering services including field service representatives, maintenance of publicationsa and technical data, sparing support and project management.

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

Canada	NATO / OTAN	Foreign / Étranger
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)

Contract Number / Numéro du contrat	
W8482-206387 Amendment 2	
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 : Remark on 10 b) On DND premises, unscreen personnel may only access public, reception zones

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?

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	B	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).

Government of Canada / Gouvernement du Canada

Contract Number / Numéro du contrat	
W8482-206387 Amendment 2	
Security Classification / Classification de sécurité	
Unclassified	

PART D - AUTHORIZATION / PARTIE D - AUTORISATION

13. Organization Project Authority / Chargé de projet de l'organisme

Name (print) - Nom (en lettres moulées)	Title - Titre	Signature	
Shawn Beaudette	MSC 7-2	BEAUDETTE, SHAWN 529	Digitally signed by BEAUDETTE, SHAWN 529 Date: 2020.12.01 12:26:14 -05'00'

Telephone No. - N° de téléphone	Facsimile No. - N° de télécopieur	E-mail address - Adresse courriel	Date
613-762-7039		Shawn.Beaudette@forces.gc.ca	2021-08-17

14. Organization Security Authority / Responsable de la sécurité de l'organisme

Name (print) - Nom (en lettres moulées)	Title - Titre	Signature	
Sasa Medjovic	Senior security analyst	MEDJOVIC SASHA 234	Digitally signed by MEDJOVIC, SASHA 234 DN: C=CA, O=GC, OU=DND-MDN, OU=Personnel, OU=INTERN, CN="MEDJOVIC, SASHA 234" Reason: I am the author of this document Location: your signing location here Date: 2021.08.20 13:50:46-04'00' Foxit PhantomPDF Version: 10.1.4

Telephone No. - N° de téléphone	Facsimile No. - N° de télécopieur	E-mail address - Adresse courriel	Date
613-996-0286		sasa.medjovic@forces.gc.ca	

15. Are there additional instructions (e.g. Security Guide, Security Classification Guide) attached?
Des instructions supplémentaires (p. ex. Guide de sécurité, Guide de classification de la sécurité) sont-elles jointes?

☑ No / Non ☐ Yes / Oui

16. Procurement Officer / Agent d'approvisionnement

Name (print) - Nom (en lettres moulées)	Title - Titre	Signature
Paul Lacoursiere	Supply Team Lead; Navigation, Sonar and Radar Systrems	

Telephone No. - N° de téléphone	Facsimile No. - N° de télécopieur	E-mail address - Adresse courriel	Date
343-551-1529		Paul.Lacoursiere@	

17. Contracting Security Authority / Autorité contractante en matière de sécurité

Name (print) - Nom (en lettres moulées)	Title - Titre	Signature
C. Jason Quade Contract Security Officer Jason.Quade@pwgsc-tpsgc.gc.ca		

- N° de télécopieur	E-mail address - Adresse courriel	Date

ANNEXE C

Appendice 1

Ministère de la Défense nationale (MDN)

Document sur les exigences relatives à la sécurité des technologies de l'information

pour le

contrat W8482-206387

HISTORIQUE DES VERSIONS

VERSION	DATE DE MODIFICATION	DÉTAILS DES MODIFICATIONS	MODIFIÉ PAR
1.0	2021-03-25	Version initiale	Capt Martineau, Dir Sécur GI
1.1	2021-03-26	Version définitive	Julie Bastarache
1.2	2021-08-13	Amendement 2, paragraph 2.2.4	Shawn Beaudette, DGMEPM
1.3	2021-08-17	Accepté l'amendement proposé au paragraphe 2.2.4. Version finale	Rob Kabano, DIM Secur

TABLE DES MATIÈRES

1. INTRODUCTION

1.1 Document sur les exigences relatives à la sécurité des technologies de l'information. Le présent document, intitulé « Document sur les exigences relatives à la sécurité des technologies de l'information (TI) pour le contrat W8482-206387 » est fourni conformément aux directives pour établir la section 11.d de la partie C du formulaire 350-103 du Secrétariat du Conseil du Trésor (SCT), lesquelles stipulent que :

> […] « le fournisseur sera-t-il tenu d'utiliser ses systèmes informatiques pour traiter, produire ou stocker électroniquement des renseignements ou des données PROTÉGÉS ou CLASSIFIÉS? » Dans l'affirmative [...] le ministère ou l'organisme client doit préciser dans un document technique distinct les exigences relatives à la sécurité des TI associées à cet achat [...].

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 W8482-206387 » est spécifique au contrat W8482-206387.

1.2 Exigences du MDN en matière de sécurité des TI. Le présent document décrit les exigences du ministère de la Défense nationale (MDN) en matière de sécurité des TI servant à stocker, à traiter et à produire les renseignements exclusifs du contrat susmentionné, dont la cote de sécurité est CONFIDENTIEL et OTAN CONFIDENTIEL ou inférieure.

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. Comme le stipulent l'énoncé des travaux (EDT) et ses annexes, l'entrepreneur est limité aux seuls renseignements non classifiés dans l'environnement de données partagé (EDP). Il lui est interdit de stocker, de traiter, de produire et de transmettre des données classifiées ou des marchandises contrôlées dans cet environnement.

1.5 Couches de protection de la sécurité. La sécurité repose sur diverses couches de protection. En d'autres termes, les exigences en matière de sécurité des TI protègent efficacement l'information lorsqu'on s'y conforme, mais à condition que d'autres mesures et politiques de sécurité les sous-tendent. Il ne faut donc réaliser des travaux en sous-traitance qu'après avoir mis en œuvre des mesures pour protéger la sécurité du matériel, ainsi que celle du personnel, des procédures, de l'information 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. D'autres renseignements portant sur la sécurité sont disponibles en ligne auprès du PSC de SPAC, du Centre de la sécurité des télécommunications (CST), du Centre canadien pour la cybersécurité (CCC) et de 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 en matière de sécurité, les autres exigences énoncées dans ce document doivent être satisfaites. Si deux exigences portent sur le même enjeu, on doit appliquer la plus stricte.

2.1.2 Lieux de travail de l'entrepreneur. L'entrepreneur doit communiquer au PSC de SPAC et à l'officier de projet (OP) du MDN tous les emplacements où il a l'intention de stocker, de traiter et de produire des renseignements exclusifs CONFIDENTIEL et OTAN CONFIDENTIEL ayant trait au présent contrat. Ces emplacements comprennent les locaux de l'entrepreneur principal ou d'un autre entrepreneur, les chantiers de construction, les emplacements de stockage de secours, les locaux de partenaires, les locaux des sous-traitants de tous niveaux, etc.

2.1.3 Exigences relatives aux emplacements. Selon le cas, une attestation de sécurité d'installation (ASI), une vérification d'organisation désignée (VOD) ou une autorisation de détenir des renseignements (ADR) doit être attribuée à tout emplacement où l'entrepreneur stocke, traite ou produit des renseignements exclusifs ayant trait au présent contrat. Le PSC de SPAC doit également attester de la sécurité des différents emplacements avant que l'entrepreneur ne soit autorisé à y stocker, traiter et produire de tels renseignements exclusifs.

2.1.4 Sécurité des émissions (EMSEC). Étant donné que le présent contrat a été évalué au niveau CONFIDENTIEL et OTAN CONFIDENTIEL, l'entrepreneur doit se conformer aux spécifications de sécurité des émissions (EMSEC), telles que décrites dans le guide ITSG-11A, Conseils relatifs à la sécurité des émissions (EMSEC), du CST/CCC. Cette publication peut être obtenue auprès du PSC de SPAC ou de l'OP du MDN.

2.2 Sécurité du matériel

2.2.1 Installations autorisées. Le stockage, le traitement et la production de renseignements exclusifs ayant trait au présent contrat ne peuvent s'effectuer que dans les installations autorisées par le PSC de SPAC. Toutes les données doivent être stockées, traitées et produites en toute sécurité, de façon à empêcher quiconque de les voir, d'y accéder ou de les manipuler.

2.2.2 Zone de sécurité du matériel. Conformément au guide pour l'établissement des zones de sécurité du matériel G1-206 de la GRC, le système d'information, appelé SI W8482-206387 dans le présent document, doit être installé et exploité dans une zone de sécurité.

2.2.3 Zone de sécurité du matériel – Liste de contrôle de l'accès. Une liste de contrôle de l'accès (LCA) régit les entrées dans la zone de sécurité. Une copie papier de cette liste doit être affichée à l'intérieur de la zone où le système d'information (SI) est installé et exploité. Il incombe à l'agent de sécurité d'entreprise (ASE) ou à l'agent remplaçant de sécurité d'entreprise (ARS) de mettre à jour cette liste lorsqu'un changement survient dans la composition du personnel autorisé à accéder à la zone de sécurité.

2.2.4 Renseignements exclusifs à l'extérieur du Canada. En vertu du présent contrat, il est permit de stocker, de traiter et de produire des renseignements exclusifs à l'extérieur du Canada, sous réserve les conditions suivantes.

2.2.4.1 Conformément à la section 9.8 du MSC, lorsqu'elles attribuent des contrats, y compris des contrats de sous-traitance, à des organisations situées à l'extérieur du Canada qui détiennent une attestation de sécurité d'installation (ASI) valide dans leur pays (entrepreneur étranger), les organisations sont tenues d'obtenir l'approbation de l'AVD canadienne pour le contrat et/ou le contrat de sous-traitance.

2.2.4.2 L'entrepreneur étranger doit respecter toutes les conditions énoncées dans le " Document sur les exigences en matière de sécurité des TI pour le contrat W8482-206387

" et dans le " Document sur les ordinateurs du périmètre aérien pour le contrat W8482-206387 ".

2.2.4.3 Toute question concernant le PSPC/CSP à l'intérieur du Canada sera traitée à l'extérieur du Canada par l'autorité de sécurité désignée canadienne (ASD canadienne).

2.2.4.4 S'il n'est pas en mesure de respecter toutes les exigences en matière de sécurité, l'entrepreneur étranger est tenu de fournir des " mesures d'atténuation proposées par rapport à des exigences précises " qui seront examinées par l'OP du MDN, puis discutées avec l'entrepreneur étranger afin de déterminer les mesures de protection acceptables pour le MDN.

2.2.5 Informatique mobile et télétravail. En vertu du présent contrat, les membres du personnel à l'emploi de l'entrepreneur n'ont pas le droit d'utiliser l'informatique mobile ou de faire du télétravail depuis leur domicile lorsqu'ils stockent, traitent ou produisent des renseignements exclusifs ou qu'ils utilisent le SI d'une manière ou d'une autre.

2.3 Sécurité du personnel

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

2.3.1.1 détenir au moins une cote de sécurité SECRET valide (niveau II) que lui accorde le PSC de SPAC et qui en assure également le suivi;

2.3.1.2 se voir attribuer les privilèges d'utilisation du système selon le critère du moindre privilège. Cela signifie qu'il faut appliquer l'ensemble de privilèges le plus restrictif et le principe du besoin de savoir (à savoir, limiter l'accès à l'information aux seules personnes qui en ont besoin dans l'exercice de leurs fonctions) nécessaires à l'exécution des tâches autorisées.

2.3.2 Accès à la zone de sécurité du matériel. Aucun visiteur, étranger ou membre du personnel non autorisé ne doit avoir accès aux renseignements exclusifs, au contrat SI W8482-206387 et à la zone où l'on stocke, traite ou produit l'information exclusive, sauf s'il détient une cote de sécurité SECRET valide (niveau II) et qu'il est accompagné par un employé autorisé de l'entrepreneur. Le nom de chaque visiteur, étranger et membre du personnel non autorisé qui entre dans la zone de sécurité doit être consigné dans un registre de vérification tenu à jour.

2.3.3 Cours de sensibilisation à la sécurité des TI. Tous les membres du personnel de l'entrepreneur qui sont en contact d'une manière ou d'un autre avec des renseignements exclusifs doivent suivre une formation ou assister à des séances d'information que coordonne l'ASE ou l'ARSE. La formation doit, à tout le moins, renvoyer au manuel de la sécurité des contrats (MSC) de SPAC et à tout autre renseignement sur la sécurité dont l'OP du MDN décidera de la pertinence, ainsi qu'aux ordonnances de sécurité et aux instructions permanentes d'opérations (IPO) relatives au système pour le contrat SI W8482-206387. La formation doit également porter sur l'ingénierie sociale, ou piratage psychologique, l'utilisation des médias sociaux et la connaissance de la situation.

2.4 Sécurité des procédures

2.4.1 Ordonnances de sécurité et instructions permanentes d'opérations relatives aux TI. L'entrepreneur doit rédiger des ordres de sécurité et des OPI ayant spécifiquement trait au SI, à son exploitation et à sa maintenance pour le contrat SI W8482-206387. Ces documents doivent, à tout le moins, fournir les renseignements suivants :

2.4.1.1 rôles et responsabilités (de l'ASE, du responsable technique, du ou des administrateurs du SI, etc.);

2.4.1.2 gestion des accès à la zone de sécurité et au système d'information (SI);

2.4.1.3 utilisation acceptable du SI;

2.4.1.4 procédures de gestion des incidents;

2.4.1.5 tout autre sujet mentionné dans le présent document;

2.4.1.6 tout autre enjeu ou problème relevé par l'OP du MDN ou le bureau de gestion de projet (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 contrat SI W8482-206387, ainsi que lire et signer le formulaire de consentement de l'utilisateur, tel que rédigé et suivi par l'ASE ou l'ARSE. Tout changement apporté aux ordonnances de sécurité des TI, aux IPO et au formulaire de consentement de l'utilisateur en lien avec le SI doit être communiqué à tous les membres du personnel qui ont accès à ce système.

2.4.3 Administrateur du système – Cote de sécurité du personnel. La ou les personnes qui assurent l'administration et la maintenance du SI doivent détenir au moins une cote de sécurité SECRET valide (niveau II).

2.4.4 Surveillance constante du SI. L'entrepreneur doit surveiller en permanence sa situation générale à l'égard de la sécurité, ce qui comprend la sécurité du matériel, du personnel, des procédures, de l'information et des TI. Il doit signaler au PSC de SPAC et à l'OP du MDN tout problème susceptible de menacer la sécurité des renseignements exclusifs ou du SI.

2.5 Sécurité de l'information

2.5.1 Marquage des documents. Que ce soit dans sa version imprimée ou électronique, tout document qui contient des renseignements exclusifs doit porter la mention du niveau de sécurité le plus élevé applicable à son contenu et un identifiant unique pour en assurer adéquatement le contrôle et le suivi.

2.5.2 Information stockée. L'entrepreneur doit protéger la sécurité des renseignements exclusifs stockés en appliquant des mesures de sécurité matérielles ou informatiques.

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 (GC). Le choix du contenant dépend du niveau de confidentialité de l'information ainsi stockée. Le ou les contenants utilisés doivent satisfaire aux exigences énoncées dans le guide d'équipement de sécurité G1-001 de la GRC. Ce guide n'étant pas destiné à la population générale, l'entrepreneur doit communiquer avec l'OP du MDN pour obtenir de l'information au sujet des contenants.

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, l'information exclusive est protégée si le support est perdu, égaré ou volé.

2.5.2.3 Seuls les membres du personnel de l'entrepreneur autorisé 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 exclusifs. Les documents imprimés ou les supports informatiques amovibles utilisés pour partager des renseignements exclusifs entre le MDN et dans l'ensemble des sociétés de l'entrepreneur et de ses sous-traitants doivent être manipulés, transportés ou expédiés conformément aux lignes directrices du GC énoncées dans le MSC ou aux directives du guide G1-009 de la GRC sur le transport et la transmission de renseignements protégés ou classifiés. Qu'il soit transporté, c'est-à-dire déplacé entre deux endroits ou entre l'expéditeur et le destinataire par une personne qui a besoin de savoir et qui détient la cote de sécurité correspondant au niveau de sécurité le plus élevé des renseignements exclusifs, ou qu'il soit expédié, c'est-à-dire envoyé à un autre endroit ou à une autre personne par un tiers, le support électronique doit être chiffré avec une technologie approuvée par le GC et correspondant au niveau de confidentialité de l'information qu'il contient.

2.5.4 Échange de renseignements exclusifs – Conditionnement. Les documents imprimés et les supports informatiques doivent être conditionnés adéquatement et transportés ou expédiés avec une lettre de présentation ainsi qu'un formulaire d'envoi ou un bordereau de circulation qui indiquent :

2.5.4.1 le niveau de confidentialité le plus élevé de l'information transportée ou expédiée;

2.5.4.2 la date du transport ou de l'expédition;

2.5.4.3 l'identifiant unique de chaque document ou support informatique transporté ou expédié;

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 municipale de 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 Mise à l'écart des renseignements exclusifs à détruire d'urgence. Tous les renseignements exclusifs (sous forme de documents imprimés, de supports informatiques, etc.) doivent à l'écart des autres renseignements contractuels et ministériels de façon que l'on puisse les détruire en toute sécurité. Dès que le PSC de SPAC ou l'OP du MDN en fait la demande, comme le précise la publication ITSP.40.006 sur le nettoyage des supports informatiques du Centre canadien pour la cybersécurité (CCC).

2.5.6 Marchandises contrôlées. Pour les besoins du présent contrat, l'entrepreneur doit avoir accès à de l'information ou à du matériel dont la cote de sécurité est CONFIDENTEL, OTAN CONFIDENTIEL et désigné marchandises contrôlées.

2.5.6.1 Toutes les données désignées marchandises contrôlées du GC (sur support papier ou électronique) doivent être marquées conformément aux Directives et ordonnances administratives de la Défense DOAD 3003-1. L'entrepreneur doit se conformer à l'ensemble des règlements sur les marchandises contrôlées du GC, y compris sur l'accès et le transfert de la technologie contrôlée (ATTC) et sur le commerce international des armes (règlement ITAR des États-Unis), s'il y a lieu. Au besoin, il peut obtenir d'autres renseignements en consultant en ligne le règlement DORD/2001-32 sur les marchandises contrôlées à l'adresse https://laws-lois.justice.gc.ca/eng/regulations/SOR-2001-32/, en s'adressant au Bureau de l'ATTC par l'intermédiaire de l'OP du MDN ou en envoyant un courriel à un responsable du Programme des marchandises contrôlées (PMC) à l'adresse dmc-cgd@tpsgc-pwgsc.gc.ca.

2.5.6.2 Si un règlement quelconque sur les marchandises contrôlées contredit l'une ou l'autre des exigences en matière de sécurité des TI énoncées dans les présentes, le règlement le plus rigoureux ou l'exigence la plus rigoureuse doit s'appliquer.

2.5.7 Sous-traitants. L'entrepreneur doit signaler à l'OP du MDN et inscrire auprès du PSC de SPAC tout partenaire et sous-traitant qui prend part à l'exécution du présent contrat. C'est à l'entrepreneur qu'incombe la responsabilité de communiquer à ses sociétés et à ses sous-traitants toutes les exigences relatives à la sécurité et de leur fournir tous les documents sur la sécurité, pertinents ou afférents au présent contrat.

2.5.8 Exigences en matière de sécurité des TI pour les contrats en sous-traitance. Toutes les exigences relatives à la sécurité des TI pour le présent contrat s'appliquent également à n'importe quel contrat donné en sous-traitance.

3. EXIGENCES MINIMALES RELATIVES À LA SÉCURITÉ DES TI

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

À la fréquence et selon le calendrier qu'établira le responsable de la sécurité des TI du MDN, le Ministère se réserve le droit d'inspecter les différentes installations de chaque entrepreneur participant au présent contrat afin d'assurer leur conformité aux exigences relatives à la sécurité des TI énoncées dans les présentes, ainsi qu'aux normes et politiques du GC en matière de prévention, de détection, d'intervention et de récupération.

3.2 Configuration du système informatique

3.2.1 Type de système. Le système d'information doit être autonome, c'est-à-dire ne dépendre d'aucun autre.

3.2.2 Type de matériel. Le matériel informatique servant à stocker, à traiter et à produire des renseignements exclusifs doit être disponible sur le marché s'il se trouve dans une zone de sécurité des messages MSEC certifiée, sinon l'entrepreneur doit utiliser du matériel TEMPEST. Quel que soit le type utilisé, le matériel doit être identifié avec le niveau de confidentialité le plus élevé des renseignements exclusifs qu'il sert à stocker, à traiter et à produire.

3.2.3 Disques durs du SI. Le matériel de traitement du SI doit être doté de disques durs amovibles. Par matériel de traitement du SI, on entend les postes de travail (ordinateurs de bureau, bloc-notes et tablettes électroniques), les serveurs, les dispositifs de stockage informatiques (stockage en réseau NAS et réseau de stockage SAN), les imprimantes, les scanneurs, etc.

3.2.4 Système d'exploitation. Le SI doit être doté d'un système d'exploitation (SE) compatible, c'est-à-dire que le fournisseur du SE doit créer les correctifs de sécurité et fournir leur version la plus récente. Ces correctifs doivent être installés périodiquement, au moins chaque mois. Le SE doit être configuré pour désactiver les processus, services et ports inutiles. Les IPO relatives au SI doivent indiquer la configuration du SE, ainsi que la fréquence à laquelle les correctifs de sécurité sont appliqués au SE et la méthode utilisée pour ce faire.

3.2.5 Logiciels antivirus et antimaliciels. Une application antivirus et antimaliciels compatible et fonctionnelle doit être installée sur chacun des postes de travail et des serveurs (s'il y a lieu). La version la plus récente des fichiers de définition de l'application antivirus et antimaliciels doit être installée périodiquement. Les IPO relatives au SI doivent décrire en détail la configuration de l'application antivirus et antimaliciels et préciser également la fréquence à laquelle les fichiers de définition sont mis à jour, ainsi que la méthode employée pour les installer. L'application antivirus et antimaliciels doit être configurée de telle sorte :

3.2.5.1 qu'elle permet aux seuls administrateurs du système d'apporter des modifications;

3.2.5.2 qu'elle analyse automatiquement tous les postes de travail et tous les serveurs du SI W8482-206387 à leur mise sous tension ou à des intervalles de temps préétablis, soit au moins une fois par semaine;

3.2.5.3 qu'elle analyse tout nouveau fichier introduit dans les postes de travail et les serveurs du SI à la recherche de code malveillant.

3.2.6 Logiciels et applications. Seules les applications requises aux fins du présent contrat doivent être installées sur le SI. Les correctifs à jour de ces applications doivent être installés et gérés au moyen d'un processus de gestion de la configuration défini. Les IPO relatives au SI doivent répertorier les applications installées, indiquer leur version et préciser le processus de gestion des correctifs employé avec chacune d'elles.

3.2.7 Journalisation et vérification. La journalisation du SE doit être active, et les fichiers journaux doivent être examinés au moins une fois par mois par les différents administrateurs du SI W8482-206387. 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 et sur ses comportements inhabituels, sur les perturbations imprévues des systèmes ou des services, sur les erreurs du système, etc. Seuls les administrateurs du système sont autorisés à modifier ou à supprimer les fichiers journaux, mais seulement si l'ASE ou l'ARSE les a autorisés à procéder. Les IPO relatives au SI doivent indiquer la fréquence à laquelle les fichiers journaux du SE sont examinés et la méthode employée pour ce faire.

3.3 Matériel informatique

3.3.1 Liste des équipements. L'entrepreneur doit tenir à jour une liste des équipements qui composent le SI. Elle doit au moins en préciser la marque, le modèle et la quantité et en fournir la description. Il doit remettre cette liste au PSC de SPAC et à l'OP du MDN qui en font la demande.

3.3.2 Modifications apportées au matériel informatique. L'entrepreneur doit informer le PSC de SPAC et l'OP du MDN de tout changement important apporté au matériel informatique du SI W8482-206387.

3.3.3 Technologie Bluetooth. Il est formellement interdit à l'entrepreneur d'intégrer la technologie Bluetooth au matériel informatique du système, tout comme utiliser cette technologie dans la zone de sécurité où le SI est installé, que ce soit en permanence ou temporairement. La seule exception à cette interdiction concerne les appareils médicaux, s'ils ont été approuvés. L'ASE doit être tenu informé de la présence de tout appareil médical Bluetooth utilisé à proximité du SI W8482-206387.

3.3.4 Sans-fil ou Wi-Fi. Il est formellement interdit à l'entrepreneur d'intégrer des capacités de communication sans fil ou Wi-Fi au SI.

3.3.5 Infonuagique. Il est formellement interdit à l'entrepreneur de recourir au service infonuagique d'un fournisseur pour stocker, traiter et produire des renseignements exclusifs.

3.3.6 Diagramme topologique. L'entrepreneur doit fournir sur demande un diagramme de la topologie du SI W8482-206387 au PSC de SPAC ou à l'OP du MDN. Le diagramme doit montrer la conception globale du système et y intégrer tout lien informatique vers d'autres entités ou toute connexion vers d'autres réseaux ou systèmes, s'ils existent.

3.3.7 Entretien et élimination du matériel informatique. L'entrepreneur doit suivre les directives fournies plus loin dans la section du présent document sur l'élimination du matériel informatique utilisé pour stocker, traiter et produire des renseignements exclusifs (soit les postes de travail, les serveurs, les imprimantes, les traceurs, les scanneurs, les photocopieurs et les appareils ou imprimantes multifonctions, etc.).

3.4 Autorisations et contrôle des accès

3.4.1 Liste des membres du personnel autorisé. L'entrepreneur doit tenir à jour la liste des personnes autorisées à accéder au SI. Il doit actualiser son contenu chaque fois qu'un changement d'effectif survient ou que changent les renseignements au sujet de l'une de ces personnes. La liste doit au moins contenir les renseignements suivants :

3.4.1.1 le nom des personnes;

3.4.1.2 leur cote de sécurité;

3.4.1.3 la date à laquelle leur cote de sécurité est échue;

3.4.1.4 le type d'accès qui leur est accordé (utilisateur, super-utilisateur, administrateur, etc.).

3.4.2 Comptes d'utilisateur

3.4.2.1 L'entrepreneur doit créer un compte d'administrateur pour chacun des administrateurs du système. Toute personne qui doit accéder au SI à la fois à titre d'administrateur et d'utilisateur ordinaire doit détenir deux comptes distincts créés dans le SI. Les comptes d'administrateur ne doivent jamais servir aux opérations quotidiennes courantes ou pour résoudre des problèmes autres qu'administratifs.

3.4.2.2 L'entrepreneur doit créer un compte pour chacun des utilisateurs et lui donner un nom ou identifiant unique. Aucun autre détenteur d'un compte ne peut utiliser ce nom ou identifiant pendant la durée de vie du système. L'entrepreneur doit configurer les comptes d'utilisateur en fonction des privilèges et de l'accès aux dossiers et fichiers dont leur détenteur a besoin pour accomplir ses tâches particulières.

3.4.2.3 Le SI ne doit contenir aucun des types de comptes suivants :

3.4.2.3.1 comptes génériques;

3.4.2.3.2 comptes d'invité;

3.4.2.3.3 comptes temporaires;

3.4.2.3.4 comptes partagés d'une façon ou d'une autre.

3.4.3 Mots de passe

3.4.3.1 Chaque compte doit être protégé par un mot de passe présentant une complexité minimale qui se décline comme suit :

3.4.3.1.1 au moins huit (8) caractères;

3.4.3.1.2 trois critères parmi les suivants :

- 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 (!, $, #, %, etc.);

3.4.3.1.3 restrictions de la durée de validité du mot de passe : au moins un (1) jour et au plus 90 jours;

3.4.3.1.4 interdiction de réutiliser l'un ou l'autre des dix (1) derniers mots de passe;

3.4.3.1.5 verrouillage du compte après quatre (4) tentatives de connexion infructueuses.

3.4.3.2 Le mot de passe utilisé pour accéder au SI doit :

3.4.3.2.1 être changé à la première ouverture de session;

3.4.3.2.2 être changé dès que l'on soupçonne qu'il a été compromis;

3.4.3.2.3 être différent des autres mots de passe de l'utilisateur pour accéder aux autres SI W8482-206387;

3.4.3.2.4 ne pas être enregistré par le SE ou par toute application à laquelle le SE accède;

3.4.3.2.5 ne jamais être partagé avec qui que ce soit.

3.4.3.3 Le mot de passe original de l'administrateur local pour accéder à un équipement informatique quelconque du SI doit être changé. Il est interdit d'utiliser les mots de passe par défaut du fournisseur de cet équipement. Lorsque le mot de passe de l'administrateur local est changé, il doit être consigné sur papier et placé dans une enveloppe scellée portant sur son rabat la signature de l'ASE, de l'ARSE 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 confidentialité des données traitées par le système.

3.4.4 Liste de contrôle des accès au SI. Tous les composants réseau (matériels ou virtuels) du SI doivent être surveillés et accessibles aux seuls membres du personnel autorisé (au moyen d'une liste de contrôle des accès [LCA], d'Active Directory, etc.).

3.4.5 Autorisations et contrôle des accès dans les IPO. Les IPO relatives au SI doivent inclure la description d'un processus d'autorisation et de contrôle des accès pour ajouter, désactiver et supprimer des comptes d'utilisateur.

3.5 Supports informatiques

3.5.1 Élimination des supports informatiques. Pour la durée du présent contrat, il faut éliminer tous les supports informatiques servant à stocker, à traiter et à produire des renseignements exclusifs, conformément aux directives fournies plus loin à la section sur l'élimination.

3.5.2 Retrait des supports informatiques. Lorsque du matériel informatique requiert un entretien, un dépannage ou un remplacement, **aucun support informatique contenant des renseignements exclusifs de quelque nature que ce soit** (disque dur, clé USB, disque optique, etc.) ne doit être remis à un fournisseur externe, à un fournisseur de services ou à un membre du personnel non autorisé ou mis à sa disponibilité.

3.5.3 Identification des supports informatiques. Tous les supports informatiques (disques durs internes, externes ou amovibles, disques optiques – CD et DVD – clés USB, etc.) servant à stocker, à traiter et à produire des renseignements exclusifs doivent :

3.5.3.1 servir uniquement aux fins du présent contrat;

3.5.3.2 recevoir un identifiant unique pour en assurer adéquatement le contrôle et le suivi;

3.5.3.3 être identifiés et répertoriés avec les renseignements suivants :

3.5.3.3.1 le type de support (disque optique, clé USB, etc.);

3.5.3.3.2 le niveau de confidentialité de l'information qu'ils contiennent;

3.5.3.3.3 toute restriction relative à la divulgation du contenu (s'il y a lieu);

3.5.3.3.4 le modèle et le numéro de série (s'ils existent);

3.5.3.3.5 l'identifiant unique du support informatique;

3.5.3.4 porter une étiquette pour indiquer :

3.5.3.4.1 le niveau de confidentialité le plus élevé des données qu'ils contiennent;

3.5.3.4.2 le nom du ministère (MDN dans le cas présent);

3.5.3.4.3 le numéro de contrat;

3.5.3.4.4 l'identifiant unique du support informatique.

3.5.3.5 S'il est impossible d'apposer une étiquette directement sur le support informatique, il faut trouver un autre moyen d'y parvenir (p. ex., avec une ficelle).

3.5.4 Protection des supports informatiques. Tous les supports informatiques doivent être protégés en fonction du niveau de confidentialité le plus élevé des données qu'ils contiennent. Lorsqu'on ne les utilise pas, les supports informatiques amovibles, y compris ceux qui sont défectueux, qui ont une durée de vie utile ou qu'on utilise à long terme (p. ex., pour les sauvegardes), doivent être rangés dans un contenant verrouillé et approuvé en fonction du niveau de confidentialité de leur contenu.

3.5.5 Ordinateur isolé du contrat. Dans l'éventualité où le SI doit interagir avec une source de données non fiable (Internet, un autre réseau, des supports informatiques d'une autre provenance, etc.), l'entrepreneur doit fournir un ordinateur autonome et isolé du contrat. L'OP du MDN doit fournir à l'entrepreneur un document technique distinct dans lequel sont établies les exigences relatives à la sécurité des transferts de données et les directives connexes se rapportant à l'ordinateur isolé. Le Dir Sécur Gi peut fournir sur demande un modèle de ce document technique.

3.5.6 Consignation des supports informatiques amovibles. L'emplacement de tous les supports informatiques amovibles doit être suivi et contrôlé au moyen d'un registre. Celui-ci doit contenir au moins les renseignements suivants :

3.5.6.1 le type de support (disque optique, clé USB, disque dur amovible, bande magnétique de sauvegarde, etc.);

3.5.6.2 l'identifiant unique du support informatique;

3.5.6.3 la date et l'heure auxquelles le support a été retiré;

3.5.6.4 le nom ou les initiales et la signature de la personne qui a emprunté le support;

3.5.6.5 la date et l'heure auxquelles le support a été rendu;

3.5.6.6 t le nom ou les initiales et la signature de la personne qui a rendu le support.

3.6 Dispositifs informatiques personnels (DIP)

3.6.1 L'entrepreneur doit veiller à ce que tous les dispositifs informatiques personnels (téléphones cellulaires, montres intelligentes, appareils FitBits, etc.) ne pénètrent pas dans la zone de sécurité où se trouve le SI W8482-206387.

3.7 Impression et reproduction de documents

3.7.1 Autorisation d'imprimer ou de reproduire. L'entrepreneur :

3.7.1.1 est autorisé à imprimer ou à reproduire des renseignements exclusifs dans ses locaux au moyen d'un appareil d'impression présent sur place et branché au SI au moyen d'un câble TEMPEST ou à fibre optique;

3.7.1.2 n'est pas autorisé à recourir aux services d'un tiers pour imprimer ou reproduire des renseignements exclusifs sans avoir obtenu au préalable l'approbation et l'autorisation du PSC de SPAC et de l'OP du MDN.

3.7.2 Disques durs des dispositifs d'impression ou de reproduction. Les appareils servant à reproduire des renseignements exclusifs (imprimantes, traceurs, scanneurs, photocopieurs, appareils ou imprimantes multifonctions, etc.) doivent être dotés de disques durs amovibles. L'entrepreneur doit substituer à un appareil qui n'est pas compatible avec la technologie des disques durs amovibles, un appareil d'un autre type sans disque dur interne ou doté d'un disque dur amovible.

3.7.3 Connexion d'imprimantes. À moins que le SI ne soit configuré comme un segment du réseau d'entreprise de l'entrepreneur, l'entrepreneur ne peut brancher les imprimantes, traceurs, scanneurs, photocopieurs et les appareils et imprimantes multifonctions qu'à ce système. Il lui est formellement interdit d'y brancher d'autres appareils ou réseaux.

3.7.4 Branchement de lignes téléphoniques. Il est formellement interdit à l'entrepreneur de brancher un nombre quelconque de lignes téléphoniques à un appareil ou une imprimante multifonctions servant à traiter des renseignements exclusifs.

3.7.5 Reproduction de renseignements exclusifs de nature particulièrement délicate. Quels que soient les renseignements exclusifs de nature particulièrement délicate que contient un document, son impression ou sa reproduction doit être approuvée au préalable par l'OP du MDN et chaque exemplaire du document doit recevoir un identifiant unique pour en assurer adéquatement le suivi et le contrôle.

3.8 Récupération

3.8.1 Sauvegarde du SI. L'entrepreneur doit sauvegarder périodiquement, soit au moins une fois par semaine, les renseignements exclusifs. Il doit ranger les copies de sécurité ainsi créées dans un autre endroit (p. ex., dans un autre édifice) afin d'en assurer la protection. Si l'entrepreneur n'a pas accès à un autre endroit pour ce faire, il peut prendre les dispositions nécessaires avec l'OP du MDN. Si les copies de sécurité doivent être confiées à la protection d'un organisme tiers, une telle modalité doit faire l'objet d'un contrat donné en sous-traitance. Les IPO relatives au SI doivent fournir tous les renseignements nécessaires ayant trait à la fréquence des sauvegardes, à la méthode employée et aux modalités du stockage.

3.8.2 Vérification des copies de sécurité. L'entrepreneur doit vérifier périodiquement les copies de sécurité. 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.

3.8.3 Plan de reprise après sinistre. L'entrepreneur doit concevoir et documenter un plan de reprise après sinistre (PRS) destiné au SI. Le plan doit fournir tous les renseignements nécessaires ayant trait à la récupération, à la restauration, à la fréquence des vérifications et à la méthode employée.

3.9 Élimination

3.9.1 Autorisation d'éliminer. L'OP du MDN doit autoriser au préalable l'élimination de tous les supports informatiques utilisés dans le cadre du présent contrat, y compris les supports amovibles et les disques durs internes et externes. Les activités d'élimination doivent être documentées et suivies. Plusieurs causes forcent l'élimination d'un support informatique, soit parce qu'il est défectueux, que sa durée de vie utile est terminée, qu'il ne sert plus, etc. S'il est impossible de retirer le ou les disques durs d'un appareil servant à stocker, à traiter et à produire de renseignements exclusifs (comme c'est le cas avec les tablettes électroniques, par exemple), l'entrepreneur doit rendre cet appareil à l'OP du MDN.

3.9.2 Élimination sur place. Il est formellement interdit à l'entrepreneur d'éliminer dans ses locaux tout support informatique ayant servi à stocker, à traiter et à produire de renseignements exclusifs.

3.9.3 Élimination des supports informatiques – Suivi. L'entrepreneur doit assurer le suivi de l'élimination des supports informatiques en remplissant un certificat de destruction (s'il y a lieu) et un formulaire de transmission et de réception des documents. Il peut obtenir les modèles de ces documents auprès de l'OP du MDN. 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. Il doit fournir ces documents au PSC de SPAC et à l'OP du MDN qui en font la demande.

3.9.4 Retour de tous les renseignements exclusifs. À la fin du contrat, l'entrepreneur doit retourner tous les renseignements exclusifs (copies papier et électroniques) à l'OP du MDN. Cela comprend tous les exemplaires imprimés des documents, ainsi que tous les supports informatiques ayant servi à stocker, à traiter et à produire des renseignements exclusifs (disques durs internes des postes de travail, des blocs-notes, des serveurs, des photocopieurs, des appareils et imprimantes multifonctions, etc.), les disques optiques au format CD ou DVD, les clés, les cartes mémoire SD, les disques durs externes, etc.). S'il est impossible de retirer le ou les disques durs d'un appareil servant à stocker, à traiter et à produire de renseignements exclusifs (comme c'est le cas avec les tablettes électroniques, par exemple), l'entrepreneur doit le rendre à l'OP du MDN. Si l'entrepreneur a utilisé des biens contrôlés, il doit les démilitariser de concert avec l'OP du MDN.

3.9.5 Procédures précédant le retrait du matériel informatique. L'entrepreneur doit suivre les procédures ci-dessous avant de procéder à la maintenance ou à l'élimination d'un équipement informatique servant à stocker, à traiter et à produire des renseignements exclusifs (serveur, poste de travail, imprimante, traceur, scanneur, appareil ou imprimante multifonctions, etc.).

3.9.5.1 Avec tout appareil utilisé pour imprimer des renseignements exclusifs Protégé B ou classifiés dans le cadre du présent contrat :

3.9.5.1.1 l'entrepreneur doit imprimer au moins 50 copies d'une page de texte entièrement non classifié pour éliminer toutes données susceptibles de rester présentes sur le tambour, les courroies ou tout autre composant interne de l'appareil d'impression;

3.9.5.1.2 l'entrepreneur doit éliminer toutes les cartouches de poudre d'imprimante laser comme il le fait avec les supports informatiques défectueux, dont la durée de vie utile est terminée ou qui ne servent plus. Une telle élimination a pour but d'empêcher tout incident lié aux cartouches dotées d'un tambour d'impression intégré sur lequel l'image d'un document imprimé pourrait persister.

3.9.5.2 L'entrepreneur doit retirer et éliminer tous les dispositifs de mémoire non volatile (disques durs internes, amovibles et externes, etc.) de la manière décrite dans la présente section.

3.9.5.3 L'entrepreneur doit effacer le contenu des dispositifs de mémoire volatile (barrettes de mémoire vive ordinaire [RAM], statique [SRAM] ou dynamique [DRAM], etc.) en coupant toutes leurs sources d'alimentation électrique pendant au moins 24 heures consécutives. Il doit s'assurer que la mémoire ne reçoit aucune forme d'alimentation électrique (par exemple, d'une pile interne ou par l'intermédiaire d'une connexion à un appareil). S'il subsiste un doute quant à la présence d'une source d'électricité alimentant la mémoire volatile d'un équipement servant à stocker, à traiter et à produire des renseignements exclusifs de nature très délicate, l'entrepreneur doit retirer cette mémoire et la faire détruire.

3.9.5.4 L’entrepreneur doit retirer les autocollants et effacer les marques de sécurité ayant trait au présent contrat ou au SI qui se trouvent sur l’appareil.

ANNEXE C

Appendice 2

Ministère de la Défense nationale (MDN)

Document sur le poste de travail isolé

pour le

contrat W8482-206387

HISTORIQUE DES VERSIONS

VERSION	DATE DE MODIFICATION	DÉTAILS DES MODIFICATIONS	MODIFIÉ PAR
1.0	25 mars 2021	Version initiale	Capt Martineau, Dir Sécur GI

Table des matières

1. INTRODUCTION

1.1 Le présent document décrit les exigences en matière de sécurité des technologies de l'information (TI) du ministère de la Défense nationale (MDN) pour le contrat W8482-206387 visant le transfert de données électroniques entre le système d'information (SI) nommé aux fins des présentes le SI W8482-206387; il est destiné à produire, à stocker et à traiter les renseignements exclusifs de ce contrat, jusqu'aux niveaux de confidentialité CONFIDENTIEL ou OTAN CONFIDENTIEL. Le présent « Document sur le poste de travail isolé pour le contrat W8482-206387 » vise à énoncer les exigences minimales en matière de sécurité des TI nécessaires à l'échange de données électroniques entre le SI et d'autres systèmes.

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 ministère de la Défense nationale (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).

1.3 Comme ce contrat pourrait exiger la saisie de données dont la source n'a pas été approuvée, un niveau de sécurité des TI supplémentaire est nécessaire afin de réduire la possibilité d'infection ou de maliciel provenant d'une source non approuvée. Ces étapes supplémentaires visent à protéger non seulement le SI W8482-206387, mais aussi d'autres SI avec lesquels ce SI échangera des renseignements. Le transfert de tous les renseignements contractuels dans le SI devra s'effectuer depuis un poste de travail isolé.

1.4 L'application des mesures de sécurité des TI énoncées dans le présent document est fondée sur l'exigence obligatoire selon laquelle il faut inspecter, évaluer et autoriser les lieux destinés au traitement, à la production ou au stockage de renseignements de niveau de confidentialité CONFIDENTIEL ou OTAN CONFIDENTIEL. SPAC ou le PSC doivent fournir cette validation.

2. EXIGENCES PRÉALABLES OBLIGATOIRES

2.1 Description

2.1.1 Un poste de travail autonome équipé d'un disque dur amovible et de deux logiciels antivirus/antimaliciels approuvés et compatibles doit être utilisé pour effectuer tous les transferts de données vers le SI. Les données électroniques transférées dans le SI ne peuvent provenir que d'un SI d'un niveau de confidentialité équivalent ou inférieur.

2.1.2 Le transfert des données électroniques dans le SI W8482-206387 doit être autorisé par écrit par le officier de projet (OP) du MDN.

2.2 Glossaire

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 W8482-206387.
Support de transfert source	Support électronique amovible (disque optique au format CD ou DVD, clé USB, carte SD, disque dur externe, etc.) qui contient le fichier source du système source. Pour le SI W8482-206387, le seul type de support source autorisé pour le transfert est le DVD-ROM.
Support de transfert cible	Support électronique amovible à utiliser pour déplacer le fichier source du poste de travail isolé W8482-206387 vers le système cible. Pour le SI W8482-206387, le seul type de support source autorisé pour le transfert est le DVD-ROM.

2.3 Matériel

2.3.1 Le poste de travail isolé doit se trouver dans la même zone de sécurité du matériel que le SI W8482-206387 et utiliser le même type d'équipement (commercial ou TEMPEST, par exemple), tel qu'énoncé à la section « Type d'équipement » du « Document sur les exigences relatives à la sécurité des technologies de l'information (TI) pour le contrat W8482-206387 ».

2.3.2 Le poste de travail isolé ne devra servir qu'à cela pendant toute la durée du contrat.

2.3.3 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 SPAC ou le PSC.

2.3.4 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 périphérique (imprimante, numériseur, etc.) ne peut être branché au poste de travail isolé.

2.3.5 Si ce n'est pas un ordinateur portatif, le poste de travail isolé doit être muni d'un disque dur amovible.

2.3.6 Le poste de travail isolé doit être installé et doit fonctionner dans la même zone de sécurité où est installé le SI W8482-206387.

2.3.7 Étiquetage. Le poste de travail isolé et le cas échéant le disque dur amovible doivent comporter une étiquette qui indique le niveau de confidentialité le plus élevé des renseignements exclusifs qui sont transférés à l'aide de cet équipement.

2.3.8 Étiquetage du support de transfert. Le support de transfert utilisé dans le poste de travail isolé doit comporter une étiquette indiquant les renseignements suivants :

2.3.8.1 le niveau le plus élevé de confidentialité des données contenues;

2.3.8.2 le ministère fédéral (dans ce cas, le MDN);

2.3.8.3 le numéro du contrat (ici, W8482-206387);

2.3.8.4 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 W8482-206387 »;

2.3.8.5 le type de support de transfert (« Support de transfert source » ou « Support de transfert cible »);

2.3.9 si ces renseignements ne peuvent pas être inscrits directement sur le support ou si une grande étiquette (4 po sur 6 po environ) ne peut pas être apposée directement sur le support, l'étiquette doit y être attachée d'une autre façon (ficelle, etc.);

2.3.10 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 de TI

2.4.1 Le poste de travail isolé doit exécuter un système d'exploitation (SE) 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 W8482-206387 ». 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/antimaliciels doivent être installés sur le poste de travail isolé de ce contrat, et ces logiciels doivent être compatibles. Le poste de travail isolé du contrat doit être en tout point conforme au paragraphe « Logiciels antivirus/antimaliciels » du « Document sur les exigences relatives à la sécurité des TI du contrat W8482-206387 ».

2.4.3 Toute autre application du poste de travail isolé du contrat doit être supprimée ou désinstallée, et aucune autre application ne peut être installée sur cet ordinateur.

2.4.4 Les fonctions d'audit du SE 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 W8482-206387 ».

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 W8482-206387 ». Les comptes partagés ou génériques sont interdits.

2.4.6 Les paragraphes suivants du « Document sur les exigences relatives à la sécurité des TI du contrat W8482-206387 » s'appliquent au poste de travail isolé, et doivent être respectés :

- Support amovible laissé sans surveillance;
- Supports de TI;
- Dispositifs informatiques personnels (DIP);
- Élimination.

2.5 PON visant le poste de travail isolé

2.5.1 Les PON du SI W8482-206387 doivent inclure les procédures et détails du présent « Document sur le poste de travail isolé, contrat W8482-206387 » pour tous les aspects applicables du poste de travail isolé.

3. PROCÉDURE DE TRANSFERT DES DONNÉES

3.1 La procédure ci-dessous doit être utilisée pour transférer des données électroniques provenant de toute source non fiable au SI.

3.2 Cette procédure de transfert des données doit être affichée près du poste de travail isolé W8482-206387.

PROCÉDURE DE TRANSFERT DES DONNÉES

1. Mettre le poste de travail isolé sous tension W8482-206387 et ouvrir une session.
2. S'assurer que les fichiers de définition des deux logiciels antivirus/antimaliciels sont à jour. Le cas échéant, faire les mises à jour nécessaires avant de passer à l'étape suivante.
3. Copier 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.), alors ce support devient le support de transfert source.
4. Étiqueter le support de transfert source et le brancher au poste de travail isolé.
5. Analyser le support de transfert source et tous les fichiers sources au moyen des deux logiciels antivirus/antimaliciels.
    a. Si un virus ou un maliciel est détecté, ARRÊTER la procédure. Nettoyer ou supprimer les fichiers conformément aux invites des logiciels antivirus/antimaliciels et informer l'agent de sécurité d'entreprise (ASE) ou l'agent remplaçant de sécurité d'entreprise (ARSE).
    b. Si aucun virus/maliciel n'est détecté, passer à l'étape suivante.
6. Copier les fichiers sources du support de transfert source sur le poste de travail isolé.
7. Débrancher le support de transfert source du poste de travail isolé.
8. Étiqueter le support de transfert source et le brancher au poste de travail isolé.
9. Copier sur le support de transfert cible les fichiers sources analysés du poste de travail isolé.
10. Débrancher le support de transfert cible du poste de travail isolé.
11. Brancher le support de transfert cible au système cible.
12. Copier les fichiers sources du support de transfert cible au système cible.
13. Confirmer 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. supprimer les fichiers sources du support de transfert cible;
    b. débrancher le support de transfert cible du système cible;
    c. supprimer les fichiers sources du poste de travail isolé.
15. Fermer la session et mettre le poste de travail isolé hors tension.

TOUS LES AUTRES TERMES ET CONDITIONS DE LA SOLLICITATION (DDP) DEMEURENT INCHANGÉS