Government of Canada / Gouvernement du Canada

Contract Number / Numéro du contrat
W8476-226536 002
Security Classification / Classification de sécurité CAN UNCLASSIFIED

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

PART A - CONTRACT INFORMATION / PARTIE A - INFORMATION CONTRACTUELLE

1. Originating Government Department or Organization / Ministère ou organisme gouvernemental d'origine	2. Branch or Directorate / Direction générale ou Direction
National Defence	ADM(MAT)/DGLEPM/DSSPM

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

LRF HHTI-LR In Service Support. The scope of this contract provides in-service support for the Laser Range Finder - Hand Held Thermal Imager - Long Range (LRF HHTI-LR) systems in terms of repair and overhaul, supply of spare parts, and the provision of miscellaneous engineering and logistic support.

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

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

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

Government of Canada / Gouvernement du Canada

Contract Number / Numéro du contrat
W8476-226536 002
Security Classification / Classification de sécurité CAN 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? on DND premises, unscreened pers. may only access public/reception zones — [✓] 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	PROTECTED PROTÉGÉ B	PROTECTED PROTÉGÉ C	CONFIDENTIAL CONFIDENTIEL	SECRET	TOP SECRET TRES SECRET
Information / Assets Renseignements / Biens		✓														
Production		✓														
IT Media / Support TI		✓														
IT Link / Lien électronique																

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

☑ No / Non ☐ Yes / Oui

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

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

☑ No / Non ☐ Yes / Oui

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

Ministère de la Défense nationale

Document sur les exigences relatives à la sécurité des TI

pour

le contrat W8476-226536 002

HISTORIQUE DES VERSIONS

VERSION	DATE DE MODIFICATION	MODIFICATIONS	MODIFIÉ PAR
Finale	2023-11-17	Mêmes exigences que W8476-226536 001. Le document a été marqué comme final.	Capt N. I. Macpherson, Dir Sécur GI

TABLE DES MATIÈRES

1. INTRODUCTION

1.1 Document sur les exigences relatives à la sécurité des TI. Le présent document, intitulé *Document sur les exigences relatives à la sécurité des TI pour le contrat W8476-226536 002* est fourni conformément aux instructions pour remplir la partie C, section 11. d), du formulaire 350-103 du Secrétariat du Conseil du Trésor (SCT) :

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

Chaque document sur les exigences relatives à la sécurité des TI ne s'applique qu'au contrat pour lequel il est rédigé. En conséquence, le présent *Document sur les exigences relatives à la sécurité des TI pour le contrat W8476-226536 002* est propre au contrat W8476-226536 002.

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 ce qui concerne la sécurité des TI servant à stocker, à traiter et à produire électroniquement les renseignements exclusifs de niveau PROTÉGÉ B, conformément aux données techniques contrôlées applicables ou inférieur du contrat susmentionné.

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 pour exécuter un contrat conclu avec le MDN, contrat dont la sécurité est assurée par l'intermédiaire du Programme de sécurité des contrats (PSC) de Services publics et Approvisionnement Canada (SPAC).

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

1.5 Couches de protection de la sécurité. La sécurité repose sur diverses couches de protection. En d'autres termes, les exigences relatives à la sécurité des TI 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 confier des travaux à des entrepreneurs qu'après avoir mis en œuvre des mesures pour assurer la sécurité du matériel, 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 doivent suivre les organisations établies au Canada pour protéger l'information et les biens du gouvernement. D'autres renseignements sur la sécurité sont accessibles sur le site Web du PSC de SPAC, ainsi que sur ceux 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. L'entrepreneur doit veiller à ce que, pendant la durée du contrat, toutes les exigences de sécurité applicables dans le MSC ainsi que toutes les exigences de sécurité du présent document soient respectées. Lorsque deux exigences se rapportent au même enjeu, la plus stricte s'applique.

2.1.2 Emplacements utilisés par l'entrepreneur. L'entrepreneur doit informer le PSC de SPAC et l'OP du MDN de tous les emplacements où il a l'intention de stocker, de traiter et de produire des renseignements exclusifs de données techniques contrôlées ayant trait au contrat. Ces emplacements comprennent tous les locaux principaux ou secondaires de l'entrepreneur, les chantiers de construction, les lieux d'entreposage de secours, les bureaux de partenaires et de 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 contrat. Le PSC de SPAC doit également attester de la sécurité de chaque emplacement avant que l'entrepreneur ne soit autorisé à y stocker, traiter et produire des renseignements exclusifs.

2.2 Sécurité du matériel

2.2.1 Installations autorisées. Le stockage, le traitement et la production des renseignements exclusifs ayant trait au contrat ne peuvent s'effectuer que dans des 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 Zones de sécurité du matériel. Conformément au *Guide pour l'établissement des zones de sécurité matérielle* G1-026 de la GRC, le SI (ci-après le « SI visé par le SI du TL ITP-LP »), doit être installé et exploité dans une zone de travail ou une zone d'opérations temporaire.

2.2.3 Renseignements exclusifs à l'extérieur du Canada. Dans le cadre du présent contrat, il est permis de stocker, de traiter et de produire des renseignements exclusifs à l'extérieur du Canada, selon les conditions ci-dessous.

2.2.3.1 L'entrepreneur étranger doit d'abord être évalué et autorisé par le PSC de SPAC et l'O Proj du MDN.

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

2.2.4.5 Toute question concernant le PSC de SPAC à l'intérieur du Canada sera traitée à l'extérieur du Canada par l'ASD canadienne.

2.2.4 Télétravail et informatique mobile. Dans le cadre du présent contrat, il est permis de faire du télétravail et d'utiliser l'informatique mobile pour effectuer des tâches liées au SI ou aux renseignements exclusifs, selon les conditions ci-dessous.

2.2.4.1 Le PSC de SPAC doit d'abord autoriser l'emplacement de télétravail ou d'informatique mobile et, s'il le juge nécessaire, l'inspecter.

2.2.4.2 L'agent de sécurité d'entreprise (ASE) de l'entrepreneur doit informer l'O Proj du MDN et le PSC de SPAC de toute violation de sécurité, de tout incident important ou de toute compromission liés au télétravail ou à l'informatique mobile.

2.2.4.3 Les activités de télétravail ou d'informatique mobile doivent être conformes en tout point à la totalité des exigences du présent document en matière de sécurité des TI.

2.2.4.4 Responsabilités de l'ASE préalables au télétravail et à l'informatique mobile. Les renseignements ci-dessous doivent être consignés et mis à la disposition de l'O Proj du MDN, sur demande. Avant qu'un employé entreprenne des activités de télétravail ou d'informatique mobile, l'ASE ou son remplaçant doit :

2.2.4.4.1 autoriser par écrit l'employé à faire du télétravail ou à utiliser l'informatique mobile;

2.2.4.4.2 vérifier que l'employé qui effectuera des activités de télétravail ou d'informatique mobile détient une attestation de sécurité valide délivrée par le PSC de SPAC (cote de fiabilité, au minimum);

2.2.4.4.3 vérifier que l'employé a suivi une séance de formation ou d'information sur la sécurité des TI, conformément aux modalités du paragraphe « Sensibilisation à la sécurité des TI » du présent document;

2.2.4.4.4 vérifier que l'employé qui effectuera des activités de télétravail ou d'informatique mobile a lu les ordonnances relatives à la sécurité des TI applicables au système et qu'il a signé un accord d'utilisation, conformément aux modalités du paragraphe « Accord d'utilisation » du présent document; l'accord d'utilisation en question doit énoncer les exigences et les restrictions applicables au télétravail et à l'informatique mobile;

2.2.4.4.5 s'assurer que le ou les emplacements physiques où les activités de télétravail ou d'informatique mobile se dérouleront (p. ex., l'employé travaillera de chez lui ou ailleurs) feront l'objet d'une évaluation des risques dans le contexte des exigences de sécurité applicables aux zones de travail temporaires, conformément aux annexes B et C du MSC, accessible à l'adresse Manuel de la sécurité des contrats – Exigences de sécurité des contrats du gouvernement du Canada – Filtrage de sécurité – Sécurité nationale – Sécurité nationale et défense – Canada.ca (tpsgc-pwgsc.gc.ca);

2.2.4.4.6 si l'employé utilise un réseau Wi-Fi pour effectuer ses activités de télétravail ou d'informatique mobile, vérifier que celui-ci est conforme à la publication *Utiliser le Wi-Fi sans compromettre la sécurité de votre organisation* (ITSAP.80.009) du CCC.

2.2.4.5 Responsabilités de l'entrepreneur. L'entrepreneur doit :

2.2.4.5.1 fournir de l'équipement de TI, qui lui appartient ou qu'il a loué, ainsi que les logiciels requis pour le contrat à chaque employé;

fournir un logiciel antivirus et antimaliciel ainsi qu'un système d'exploitation géré par l'entrepreneur et installer un outil de chiffrement de disque dur ou de dispositif de stockage conforme aux normes FIPS 140-2 ou 140-3 (p. ex., Bitlocker ou VeraCrypt) au moyen d'identifiants d'administrateur distincts sous le contrôle de l'équipe de TI de l'entrepreneur; l'équipement informatique ne doit pas contenir de comptes génériques, invités, temporaires ou partagés de quelque nature que ce soit;

2.2.4.5.2 veiller à ce que l'équipement de TI soit configuré de manière à n'utiliser que des technologies d'accès à distance sécurisé ou de réseau privé virtuel (RPV) avec des protocoles de chiffrement modernes (tels que TLS 1.3 ou IKEv2), conformément aux publications *Conseils sur la configuration sécurisée des protocoles réseau* (ITSP.40.062) et *Algorithmes cryptographiques pour l'information NON CLASSIFIÉ, PROTÉGÉ A et PROTÉGÉ B* (ITSP.40.111) du CCC;

2.2.4.5.3 s'assurer que les employés qui effectuent des activités de télétravail ou d'informatique mobile sont en mesure de ranger l'équipement en toute sécurité sur leur lieu de travail lorsqu'ils ne l'utilisent pas et, si ce n'est pas le cas, leur fournir les moyens de le faire;

2.2.4.5.4 fournir des supports informatiques amovibles (p. ex., clés USB ou CD/DVD) lui appartenant aux employés qui effectuent des activités de télétravail ou d'informatique mobile, si l'utilisation de tels supports est permise dans le cadre du présent contrat.

2.2.4.5.5 L'entrepreneur principal doit s'assurer que tous les employés concernés et tous les sous-traitants embauchés pour exécuter une partie du contrat respectent la totalité des exigences relatives aux activités de télétravail ou d'informatique mobile (normalement par la signature d'une politique d'utilisation acceptable de l'équipement de TI à jour).

2.2.4.6 Responsabilités des employés effectuant des activités de télétravail ou d'informatique mobile. Les employés qui utilisent de l'équipement de télétravail ou d'informatique mobile :

2.2.4.6.1 doivent cesser de travailler immédiatement et communiquer avec leur ASE ou son remplaçant s'ils ne sont pas en mesure de se conformer aux exigences en matière de sécurité énoncées dans le présent document, ou s'ils ont connaissance d'une violation de sécurité, d'un incident important ou d'une compromission des renseignements exclusifs;

2.2.4.6.2 doivent veiller à ce que l'équipement de télétravail et d'informatique mobile et les supports de stockage amovibles autorisés soient rangés de façon sécuritaire lorsqu'ils ne sont pas utilisés, comme l'indique le MSC. Si un employé effectuant des activités de télétravail ou d'informatique mobile ne dispose pas des outils ou des moyens nécessaires pour ranger l'équipement informatique et les supports de stockage amovibles autorisés de façon sécuritaire sur son lieu de travail, l'entrepreneur doit les lui fournir;

2.2.4.6.3 ne sont pas autorisés à stocker, à traiter ou à produire des renseignements exclusifs sur de l'équipement de TI ou des supports informatiques amovibles personnels;

2.2.4.6.4 ne sont pas autorisés à stocker, à traiter, à produire, à envoyer ou à recevoir des courriels contenant des renseignements exclusifs sur le téléphone intelligent fourni par l'entrepreneur, à moins d'y être expressément autorisés par écrit par l'O Proj du MDN;

2.2.4.6.5 ne sont pas autorisés à connecter l'équipement de télétravail ou d'informatique mobile à un réseau Wi-Fi public, non chiffré ou ouvert;

2.2.4.6.6 doivent s'assurer que le chiffrement du réseau Wi-Fi personnel qu'ils utilisent pour effectuer leurs activités de télétravail ou d'informatique mobile est conforme aux normes du GC et qu'il le demeure tout au long des activités en question;

2.2.4.6.7 doivent uniquement utiliser des supports informatiques amovibles fournis par l'entrepreneur (si l'utilisation de supports informatiques amovibles est autorisée).

2.2.4.7 Responsabilités de l'entrepreneur et des employés effectuant des activités de télétravail ou d'informatique mobile.

2.2.4.7.1 L'entrepreneur et les employés qui effectuent des activités de télétravail ou d'informatique mobile :

2.2.4.7.1.1 doivent s'assurer que le logiciel antivirus et antimaliciel, le système d'exploitation et les autres applications compatibles installés sur l'équipement de télétravail et d'informatique mobile sont mis à jour périodiquement et que les correctifs nécessaires sont appliqués;

2.2.4.7.1.2 devraient utiliser l'authentification multifacteur pour relier l'équipement de télétravail et d'informatique mobile au réseau de l'entrepreneur, conformément à la publication *Sécurisez vos comptes et vos appareils avec une authentification multifacteur* (ITSAP.30.030) du CCC;

2.2.4.7.1.3 doivent suivre les lignes directrices énoncées dans la publication *Annexe 2 – Conception de haut niveau – Connexion utilisateur sans fil/réseau câblé* (ITSG-41) du CCC. D'autres recommandations sont fournies dans les publications *Utiliser le Wi-Fi sans compromettre la sécurité de votre organisation* (ITSAP.80.009) et *Les réseaux privés virtuels* (ITSAP.80.101) du CCC.

2.2.4.7.2 Lorsque des renseignements exclusifs sont traités en télétravail ou au moyen de l'informatique mobile, le support informatique (support amovible, disque dur interne, etc.) doit être chiffré avec la technologie de chiffrement la plus à jour approuvée par le GC pour le niveau de confidentialité des renseignements traités. Le chiffrement utilisé doit être tenu à jour pendant toute la durée du contrat. La publication *Algorithmes cryptographiques pour l'information NON CLASSIFIÉ, PROTÉGÉ A et PROTÉGÉ B* (ITSP.40.111) fournit des renseignements sur le chiffrement.

2.2.4.7.3 L'entrepreneur et ses employés qui effectuent des activités de télétravail ou d'informatique mobile doivent lire les publications *Conseils de sécurité pour les organisations dont les employés travaillent à distance* (ITSAP.10.016) et *Conseils de cybersécurité pour le télétravail* (ITSAP.10.116) du CCC et en suivre les recommandations.

2.2.4.8 Renseignements requis sur les employés effectuant des activités de télétravail ou d'informatique mobile. Pour chaque employé effectuant des activités de télétravail ou d'informatique mobile, l'entrepreneur doit consigner les renseignements ci-dessous et les fournir à l'O Proj du MDN sur demande :

2.2.4.8.1 le niveau de sensibilité le plus élevé des données qui seront traitées par l'employé effectuant des activités de télétravail ou d'informatique mobile (PROTÉGÉ B au maximum);

2.2.4.8.2 le type d'équipement de TI qui sera utilisé (p. ex., client léger [terminal passif] ou client lourd [ordinateur de bureau, ordinateur portatif, tablette, etc.]);

2.2.4.8.3 le type de compte qui sera utilisé (p. ex., compte d'utilisateur normal, compte avec privilèges ou compte de groupe);

2.2.4.8.4 la façon dont les renseignements exclusifs seront téléchargés vers et depuis l'équipement de TI (par connexion RPV ou, si l'utilisation de supports amovibles est autorisée, au moyen de clés USB, de CD/DVD, etc.);

2.2.4.8.5 le type de chiffrement utilisé pour le disque dur et les supports amovibles, ou la protection par mot de passe des fichiers de données individuels, notamment le type et le niveau de chiffrement qui seront utilisés, ainsi que la méthode d'accès au RPV;

2.2.4.8.6 le ou les emplacements physiques où les activités de télétravail ou d'informatique mobile se dérouleront (p. ex., l'employé travaillera de chez lui ou ailleurs);

2.2.4.8.7 les renseignements suivants sur tous les dispositifs de TI que l'employé utilisera pour effectuer ses activités de télétravail ou d'informatique mobile : le type et le nombre de dispositifs, la marque, le modèle et l'année de fabrication.

L'entrepreneur et ses employés qui effectuent des activités de télétravail ou d'informatique mobile doivent lire les publications *Conseils de sécurité pour les organisations dont les employés travaillent à distance* (ITSAP.10.016) et *Conseils de cybersécurité pour le télétravail* (ITSAP.10.116) du CCC et en suivre les recommandations.

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 doivent :

2.3.1.1 détenir au moins une COTE DE FIABILITÉ valide accordée et tenue à jour par le PSC de SPAC;

2.3.1.2 se voir attribuer des privilèges 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 (c.-à-d. limiter l'accès aux renseignements 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, ressortissant étranger ou membre du personnel non autorisé ne doit avoir accès aux renseignements exclusifs, au SI du TL ITP-LP ou à la zone de stockage, de traitement et de production des renseignements exclusifs, sauf s'il détient une COTE DE FIABILITÉ valide et qu'il est accompagné par un employé autorisé de l'entrepreneur.

2.3.3 Séances de sensibilisation à la sécurité des TI. Tous les membres du personnel de l'entrepreneur qui traitent des renseignements exclusifs doivent suivre des séances de formation ou d'information coordonnées par l'agent de sécurité d'entreprise (ASE) ou son remplaçant. La formation doit, à tout le moins, renvoyer au MSC de SPAC et à tout autre document sur la sécurité jugé pertinent par l'OP du MDN, ainsi qu'aux ordonnances de sécurité des TI et aux instructions permanentes d'opérations (IPO) propres au SI du TL ITP-LP. Les séances doivent également porter sur l'ingénierie sociale, l'utilisation des médias sociaux et la connaissance de la situation.

2.4 Sécurité des procédures

2.4.1 Ordonnances de sécurité des TI et instructions permanentes d'opérations. L'entrepreneur doit rédiger des ordonnances de sécurité des TI et des IPO pour le SI du TL ITP-LP, à son exploitation et à sa maintenance. Ces IPO doivent être tenues à jour et demeurer à la disposition du personnel autorisé chargé d'examiner ou de réviser le document. Ces documents doivent, à tout le moins, traiter des éléments suivants :

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

2.4.1.2 la gestion des accès à la zone d'opérations et au SI du TL ITP-LP;

2.4.1.3 la politique d'utilisation acceptable du SI du TL ITP-LP;

2.4.1.4 la méthode utilisée pour mettre à jour les correctifs de sécurité du système d'exploitation (SE) et la fréquence des mises à jour et donner des précisions sur la configuration du SE;

2.4.1.5 les renseignements sur les procédures de gestion des incidents de TI;

2.4.1.6 la méthode utilisée pour mettre à jour les fichiers de définition antivirus, la fréquence des mises à jour et la configuration du logiciel antivirus/de l'antimaliciel;

2.4.1.7 la liste de toutes les applications installées, y compris les numéros de version, ainsi que le processus de gestion des correctifs d'application;

2.4.1.8 la méthode utilisée pour examiner les fichiers de journalisation du SE, la fréquence des examens et le personnel chargé de cette tâche;

2.4.1.9 le processus d'autorisation et de contrôle de l'accès décrivant le processus d'ajout et de suppression des utilisateurs (pour plus de renseignements, consultez la publication « Guide sur l'authentification des utilisateurs dans les systèmes de technologie de l'information [ITSP.30.031 v3] »);

2.4.1.10 les détails sur les copies de sauvegardes (p. ex., la fréquence, la méthodologie, le stockage);

2.4.1.11 tout autre sujet mentionné dans le présent document;

2.4.1.12 toute autre question soulevée par l'OP ou le bureau de gestion de projet (BGP) du MDN durant la période de validité du présent contrat.

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

2.4.3 Administrateur du système – Cote de sécurité du personnel. L'administration et la maintenance du SI doivent être assurées à l'interne par une ou des personnes qui possèdent, à tout le moins, une cote de sécurité de niveau SECRET (niv. II) valide.

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

2.4.5 Surveillance continue du SI. L'entrepreneur doit 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 des renseignements

2.5.1 Marquage des documents. Qu'ils soient imprimés ou électroniques, tous les documents qui contiennent des renseignements exclusifs doivent porter la mention du niveau de sécurité le plus élevé applicable à leur contenu et se voir attribuer un identifiant unique permettant d'en assurer adéquatement le contrôle et le suivi.

2.5.2 Renseignements stockés. L'entrepreneur doit assurer 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 de renseignement doivent être rangés dans des contenants sécurisés et verrouillés approuvés par le GC pour le niveau de sensibilité des renseignements. 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 peut communiquer avec l'OP du MDN pour obtenir de l'information au sujet des contenants.

2.5.2.2 Lorsqu'ils sont laissés sans surveillance, tous les supports informatiques amovibles utilisés pour conserver, traiter ou produire des renseignements exclusifs doivent être chiffrés avec une technologie approuvée par le GC et correspondant

au niveau de sensibilité des renseignements qu'ils contiennent. De cette façon, les renseignements exclusifs sont protégés si le support est perdu, égaré ou volé.

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

2.5.3 Échange de renseignements exclusifs. Tous les documents imprimés et tous les supports informatiques utilisés pour échanger des renseignements exclusifs entre le MDN et l'ensemble des sociétés de l'entrepreneur et de ses sous-traitants doivent être manipulés, transportés ou expédiés conformément aux lignes directrices énoncées dans le MSC du GC ou dans le guide *Transport et transmission de renseignements protégés ou classifiés* G1-009 de la GRC. 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 sensibilité des renseignements 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 sensibilité le plus élevé des renseignements transportés ou expédiés;

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 être mis à l'écart des autres renseignements contractuels et ministériels de façon à ce que l'on puisse les détruire ou les effacer en toute sécurité dès que le PSC de SPAC ou l'OP du MDN en fait la demande, comme le précise la publication *Nettoyage des supports informatiques* (ITSP.40.006) du CST.

2.5.6 Marchandises contrôlées. Les contrats portant sur des marchandises contrôlées doivent à tout le moins traiter leurs renseignements électroniques comme étant de niveau PROTÉGÉ B et communiquer avec le Bureau de l'ATTC (accès et transfert de la technologie contrôlée) à l'adresse CTATProgramandCompliance-

ATTCProgrammeetConformite@forces.gc.ca pour connaître les exigences supplémentaires en matière de sécurité.

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 partenaires 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

3.1.1 Conformité et surveillance. 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 utilisées par l'entrepreneur dans le cadre du présent contrat afin de vérifier 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 de TI

3.2.1 Configuration du système de base. D'après l'O Proj du MDN, le système de base devrait être configuré comme un réseau de serveurs, de postes de travail (ordinateurs de bureau, ordinateurs portatifs ou tablettes électroniques), d'imprimantes, d'appareils multifonctions et de numériseurs. Il pourrait prendre la forme d'un tout nouveau réseau ou celle d'un segment d'un réseau de l'entrepreneur. Les renseignements pourraient être téléversés et téléchargés au moyen de supports amovibles (CD/DVD, clés USB, etc.). Ce réseau pourrait être connecté à Internet.

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

3.2.3 Séparation du SI. Si le SI est configuré comme un segment du réseau de l'entrepreneur, ce dernier doit séparer son réseau en zones de sécurité de TI et mettre en place des mesures de défense du périmètre et de sécurité du réseau. Voir les lignes directrices du CST et du CCC à ce sujet : *Considérations de conception relatives au positionnement des services dans les zones* (ITSG-38) et *Exigences de base en matière de sécurité pour les zones de sécurité de réseau au sein du gouvernement du Canada* (ITSG-22). La méthodologie utilisée pour séparer le réseau (c.-à-d. le diagramme topologique et les autres documents jugés nécessaires) doit être soumise à l'évaluation du PSC de SPAC et de l'OP du MDN.

3.2.4 Type d'équipement. L'équipement servant à stocker, à traiter et à produire des renseignements exclusifs doit être composé de produits commerciaux et doit être identifié selon le niveau de sensibilité le plus élevé des renseignements exclusifs qu'il sert à traiter. Par équipement de traitement du SI, on entend les postes de travail (ordinateurs de bureau, ordinateurs portatifs et tablettes électroniques), les serveurs, les dispositifs de stockage informatiques (stockage en réseau NAS et réseau de stockage SAN), les imprimantes, les numériseurs, etc.

3.2.5 Disques durs du SI. L'équipement de traitement du SI peut être doté de disques durs internes, | amovibles | et/ou externes.

3.2.6 Système(s) d'exploitation. Tout l'équipement de TI utilisé dans le cadre du SI du TL ITP-LP doit être doté d'un SE compatible, c'est-à-dire que le fournisseur du système d'exploitation doit créer les correctifs de sécurité nécessaires et fournir leur version la plus récente. Ces correctifs doivent être installés périodiquement, au moins chaque mois. Le système d'exploitation doit être renforcé, c'est-à-dire qu'il doit être configuré pour désactiver les processus, services et ports inutiles. Les IPO relatives au SI doivent indiquer la configuration du système d'exploitation, la fréquence à laquelle les correctifs de sécurité sont appliqués au système d'exploitation, ainsi que la méthode utilisée pour ce faire.

3.2.7 Logiciels antivirus et antimaliciels. Une application antivirus et antimaliciel compatible et fonctionnelle doit être installée sur tout l'équipement de TI applicable. La version la plus récente des fichiers de définition de l'application antivirus et antimaliciel doit être installée périodiquement. Les IPO relatives au SI doivent décrire la fréquence et la méthode utilisée pour mettre à jour les fichiers de définition antivirus et antimaliciels ainsi que la configuration du logiciel antivirus. L'application antivirus et antimaliciel doit être configurée de telle sorte :

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

3.2.7.2 qu'elle analyse automatiquement tout l'équipement de TI visé par le SI du TL ITP-LP à leur mise sous tension ou à des intervalles de temps préétablis, soit au moins une fois par semaine;

3.2.7.3 qu'elle analyse tout nouveau fichier introduit dans les postes de travail et les serveurs du SI visé par le SI du TL ITP-LP à la recherche de code malveillant.

3.2.8 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. Les exigences et recommandations de sécurité minimales concernant l'accès par le Web (HTTPS) à un environnement collaboratif (EC) à authentification unique pour l'échange de renseignements exclusifs du MDN et des FAC de niveau Protégé B ou inférieur dans le cadre du présent contrat sont les suivantes :

3.2.8.1 S'assurer que le site Web utilise le protocole de transfert hypertexte sécurisé (HTTPS) pour une communication sécurisée (chiffrée) avec le protocole Transport Layer Security (TLS) le plus récent, tel que TLS 1.2 ou 1.3. Suivre les lignes directrices du document NIST SP 800-95 sur les services Web sécurisés et celles des documents NIST SP 800-175A, SP 800-175B rév. 1, FIPS 140-2 et FIPS 186-4 sur le chiffrement des services Web.

3.2.8.2 Planifier des audits de sécurité du site Web pour trouver et corriger les vulnérabilités. Des mesures de sécurité devraient être mises en œuvre au niveau de l'application Web afin de prévenir les 10 problèmes de sécurité les plus importants (OWASP), c'est-à-dire l'injection, l'authentification de mauvaise qualité, l'exposition de données sensibles, les entités externes XML (XXE), le contrôle d'accès défaillant, la mauvaise configuration de sécurité, les scripts intersites (XSS), la désérialisation non sécurisée, l'utilisation de composants présentant des vulnérabilités connues, ainsi que la journalisation et la supervision insuffisantes.

3.2.8.3 Mettre à jour le site Web ou le logiciel de façon périodique.

3.2.8.4 Installer des modules de sécurité externes et les tenir à jour.

3.2.8.5 Utiliser un système de sauvegarde automatique pour le site Web.

3.2.8.6 Établir une méthode d'authentification par mot de passe ou clé publique/privée.

3.2.8.7 Appliquer des mots de passe robustes et les modifier régulièrement.

3.2.8.8 Déployer l'authentification à deux facteurs pour accéder au site Web.

3.2.8.9 Créer des niveaux d'accès, limiter l'accès aux parties du site Web que les employés doivent utiliser pour accomplir leurs tâches quotidiennes, accorder seulement les privilèges nécessaires.

3.2.8.10 Déployer un pare-feu d'application Web (WAF).

3.2.8.11 Choisir un fournisseur d'hébergement Web qui offre des services de surveillance du réseau en tout temps et une protection par pare-feu contre toutes les menaces connues.

3.2.8.12 Utiliser les meilleures pratiques du cadre de développement de logiciels sécurisés (SSDF) pour atténuer le risque de vulnérabilités logicielles, conformément au livre blanc du NIST, accessible à l'adresse https://doi.org/10.6028/NIST.CSWP.04232020.

3.2.8.13 Obtenir les certifications ou attestations de conformité appropriées pour les applications Web et les API qui traiteront des données sensibles telles que des données financières (PCI DSS), des données de santé (HIPAA) et des renseignements permettant d'identifier une personne (PII) afin de s'assurer que ces données sont protégées (chiffrées) lorsqu'elles sont utilisées, en transit et stockées.

3.2.10 Journalisation et vérification. La fonction de journalisation du système d'exploitation doit être activée, et le ou les administrateurs du SI du TL ITP-LP doivent examiner les fichiers journaux au moins une fois par trimestre ou chaque fois qu'ils soupçonnent une compromission. Cet examen doit porter notamment sur les ouvertures de session réussies et infructueuses, sur les modifications non autorisées apportées au matériel, au micrologiciel et aux logiciels du système, sur les comportements inhabituels du système, sur les perturbations imprévues des systèmes ou des services, sur les erreurs du système, etc. Seuls les administrateurs du système sont autorisés à modifier ou à supprimer les fichiers journaux, mais seulement si l'ASE ou son remplaçant les a autorisés à procéder. Les IPO relatives au SI doivent indiquer la fréquence à laquelle les fichiers journaux du système d'exploitation sont examinés et la méthode employée pour ce faire.

3.3 Équipement de TI

3.3.1 Liste de l'équipement. L'entrepreneur doit tenir une liste de tout l'équipement qui compose le SI. Cette liste doit au moins préciser la marque, le modèle et la quantité d'équipement et en fournir la description. L'entrepreneur doit remettre cette liste au PSC de SPAC et à l'OP du MDN s'ils en font la demande.

3.3.2 Modifications apportées à l'équipement de TI. L'entrepreneur doit informer le PSC de SPAC et l'OP du MDN de toute modification importante apportée à l'équipement de TI du SI du TL ITP-LP.

3.3.3 Technologie Bluetooth. Il est formellement interdit d'utiliser la technologie Bluetooth avec l'équipement de TI du SI. L'utilisation de la technologie Bluetooth dans la zone d'opérations ou la zone d'opérations temporaire où se trouve le SI est strictement interdite, sauf dans le cas de dispositifs médicaux approuvés; l'ASE doit être informé de tout dispositif médical Bluetooth utilisé à proximité du SI du TL ITP-LP et doit autoriser l'utilisation de ce dispositif par écrit.

3.3.4 Sans fil ou Wi-Fi. L'utilisation de capacités de communication sans fil ou Wi-Fi avec le SI est permise dans les conditions suivantes :

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

3.3.4.2 Les capacités de communication sans fil ou Wi-Fi peuvent être utilisées dans les locaux de l'entrepreneur dans les conditions suivantes :

3.3.4.2.1 Les connexions sans fil ou Wi-Fi au SI doivent être chiffrées. L'utilisation du protocole WPA2 est suggérée; on exige le chiffrement à 128 bits au minimum, mais le chiffrement à 256 bits est fortement encourage.

3.3.4.2.2 L'entrepreneur doit établir des restrictions d'utilisation, y compris des mécanismes d'application des droits d'accès; seul le personnel autorisé se verra attribuer un compte d'accès au réseau sans fil ou Wi-Fi.

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

3.3.4.2.4 Les utilisateurs ne sont pas autorisés à modifier les paramètres du réseau sans fil ou Wi-Fi; toute modification doit être effectuée par le ou les administrateurs du système et seulement avec l'accord écrit de l'O Proj du MDN.

3.3.4.2.5 Les capacités de communication sans fil ou Wi-Fi qui seront utilisées pour stocker, traiter ou produire des renseignements exclusifs dans les locaux de l'entrepreneur doivent d'abord être validées, inspectées et autorisées par le PSP de SPAC.

3.3.5 Technologie infonuagique. Il est autorisé d'utiliser la technologie infonuagique publique ou de tiers pour stocker, traiter et produire des renseignements exclusifs dans les conditions suivantes :

3.3.5.1 L'entrepreneur n'est autorisé à utiliser que le service infonuagique Connexion de Postes Canada.

3.3.6 Interconnexion de réseau. Les connexions de l'équipement au SI :

3.3.6.1 peuvent être réalisées au moyen de câbles CAT 6 ou d'une connexion sans fil/Wi-Fi;

3.3.6.2 doivent pouvoir se différencier de toute autre connexion du système;

3.3.6.3 doivent faire l'objet d'un contrôle et d'une surveillance visant à empêcher toute connexion accidentelle ou délibérée à une infrastructure, un réseau ou de l'équipement non autorisé;

3.3.6.4 peuvent être logées dans une infrastructure de câblage d'entreprise standard.

3.3.7 Diagramme topologique. L'entrepreneur doit fournir sur demande un diagramme de la topologie du SI du TL ITP-LP 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.

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

3.4 Autorisations et contrôle des accès

3.4.1 Liste des membres du personnel autorisés. L'entrepreneur doit tenir une liste des personnes autorisées à accéder au SI. Il doit actualiser son contenu chaque fois qu'un changement d'effectif survient ou que les renseignements au sujet de l'une de ces personnes changent. 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 la cote de sécurité arrive à échéance;

3.4.1.4 le type de compte qui est accordé (utilisateur, superutilisateur, lecture du journal des événements, administrateur, etc.).

3.4.2 Comptes du système.

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 un identifiant unique. Aucun autre détenteur de compte ne peut utiliser ce nom ou cet 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 (de 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 (10) 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 à n'importe quel autre SI du contrat W8476-226536 002;

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

3.4.3.2.5 ne jamais être divulgué à qui que ce soit.

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

3.4.4 Liste de contrôle des accès au SI. Tous les composants réseau (matériels ou virtuels) du SI doivent être surveillés et accessibles aux seuls membres du personnel autorisés (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, tous les supports informatiques servant à stocker, à traiter et à produire des renseignements exclusifs doivent être éliminés conformément aux directives fournies plus loin dans la section sur l'élimination.

3.5.2 Retrait des supports informatiques. Lorsque de l'équipement requiert une maintenance, un dépannage ou un remplacement, **aucun support informatique contenant des renseignements exclusifs de quelque nature que ce soit** (disque dur interne, support amovible, etc.) ne doit être remis ou rendu accessible à un fournisseur externe, à un fournisseur de services ou à un membre du personnel non autorisé.

3.5.3 Identification des supports informatiques. Tous les supports informatiques (disques durs internes, externes ou amovibles, CD/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 permettant d'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 (CD/DVD, clé USB, etc.);

3.5.3.3.2 le niveau de sensibilité des renseignements 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 indiquant :

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

3.5.3.4.2 le nom du ministère (en l'occurrence, le MDN);

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 sensibilité le plus élevé des données qu'ils contiennent. Lorsqu'ils ne sont pas utilisés, 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 sensibilité de leur contenu.

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

3.5.5.1 le type de support (CD/DVD, clé USB, disque dur amovible, bande magnétique de sauvegarde, etc.);

3.5.5.2 l'identifiant unique du support informatique;

3.5.5.3 la date et l'heure auxquelles le support a été retiré de son conteneur de sécurité approuvé par le GC;

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

3.5.5.5 la date et l'heure auxquelles le support a été replacé dans son conteneur de sécurité approuvé par le GC;

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

3.5.6 Ordinateur isolé. L'entrepreneur n'a pas à fournir d'ordinateur autonome isolé puisque le SI du TL ITP-LP n'a pas à interagir avec des sources de données non fiables (Internet, un autre réseau, des supports informatiques amovibles d'une autre provenance, etc.).

3.6 Impression ou reproduction de documents

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

3.6.1.1 est autorisé à imprimer ou à reproduire des renseignements exclusifs dans ses locaux;

3.6.1.2 est autorisé à recourir aux services d'un tiers pour imprimer ou reproduire des renseignements exclusifs.

Le recours aux services d'un tiers pour imprimer ou reproduire des renseignements exclusifs doit d'abord être approuvé par le PSC de SPAC et l'OP du MDN.

3.6.2 Disques durs des dispositifs d'impression ou de reproduction. Les appareils utilisés pour reproduire des renseignements exclusifs (imprimantes, traceurs, numériseurs, photocopieurs, appareils ou imprimantes multifonctions, etc.) peuvent être dotés de disques durs internes et/ou amovibles.

3.6.3 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 connecter les imprimantes, traceurs, numériseurs, photocopieurs et appareils et imprimantes multifonctions qu'à ce système. Il lui est formellement interdit de les connecter à d'autres appareils ou réseaux.

3.6.4 Branchement de lignes téléphoniques. Il est formellement interdit de brancher des lignes téléphoniques sur un appareil ou une imprimante multifonctions servant à traiter des renseignements exclusifs.

3.6.5 Reproduction de renseignements exclusifs de nature particulièrement délicate. L'impression ou la reproduction d'un document contenant des renseignements exclusifs de nature particulièrement délicate doit être approuvée au préalable par l'OP du MDN, et chaque exemplaire du document doit recevoir un identifiant unique permettant d'en assurer adéquatement le suivi et le contrôle.

3.7 Récupération

3.7.1 Sauvegardes 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 (c'est-à-dire un emplacement différent qui ne risque pas d'être affecté par le même incident, tel qu'un incendie ou une inondation, qui pourrait affecter l'emplacement principal) 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.

3.7.2 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.

3.7.3 Plan de reprise après sinistre. L'entrepreneur doit concevoir et documenter un plan de reprise après sinistre (PRS) destiné au SI. Ce 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.

3.8 Élimination

3.8.1 Autorisation d'élimination. 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 des renseignements exclusifs (comme c'est le cas avec les tablettes électroniques, par exemple), l'entrepreneur doit rendre l'appareil à l'OP du MDN.

3.8.2 Élimination sur place. L'élimination sur place dans les installations de l'entrepreneur de tout support informatique utilisé pour stocker/traiter/produire des renseignements exclusifs est autorisée dans les conditions suivantes :

3.8.2.1 l'entrepreneur doit posséder de l'équipement d'élimination approuvé pour les renseignements de niveau PROTÉGÉ B, conformément aux données techniques contrôlées applicables selon le *Guide d'équipement de sécurité* G1-001 de la GRC;

3.8.2.2 l'entrepreneur doit éliminer les supports informatiques conformément à la publication *Nettoyage des supports de TI* (ITSP.40.006) du CST;

3.8.2.3 s'il ne dispose pas des moyens nécessaires pour procéder à l'élimination des supports informatiques, l'entrepreneur doit prendre les dispositions nécessaires à cette fin avec l'O Proj du MDN.

S'il est interdit d'éliminer des supports informatiques dans les locaux de l'entrepreneur, ce dernier doit prendre les dispositions nécessaires à cette fin avec l'OP du MDN.

3.8.3 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 :

3.8.3.1 envoyer une copie de ces documents au PSC de SPAC à l'adresse tpsgc.dgsssiprojetintl-dobissintlproject.pwgsc@tpsgc-pwgsc.gc.ca;

3.8.3.2 fournir ces documents à l'OP et au BGP du MDN sur demande.

3.8.4 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 ordinateurs portatifs, des serveurs, des photocopieurs, des appareils et imprimantes multifonctions, etc., les disques optiques au format CD ou DVD, les clés USB, 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 des renseignements exclusifs (comme c'est le cas avec les tablettes électroniques, par exemple), l'entrepreneur doit rendre l'appareil à l'OP du MDN.

3.8.5 Procédures précédant le retrait de l'équipement de TI. L'entrepreneur doit suivre les procédures ci-dessous avant de procéder à la maintenance ou à l'élimination d'un équipement de TI servant à stocker, à traiter et à produire des renseignements exclusifs (serveur, poste de travail, imprimante, traceur, numériseur, appareil ou imprimante multifonctions, etc.). Ces procédures s'appliquent à tout l'équipement de TI contenant des supports informatiques.

3.8.5.1 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.

3.8.5.2 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.

3.8.5.3 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.

EXIGENCE EN MATIÈRE DE SÉCURITÉ POUR ENTREPRENEUR CANADIEN:
DOSSIER TPSGC Nº W8476-226536-002

1. L'entrepreneur doit détenir en permanence, pendant l'exécution du contrat, une attestation de vérification d'organisation désignée (VOD) en vigueur, et obtenir une cote de protection des documents et de production approuvées au niveau PROTÉGÉ B, délivrées par le Programme de sécurité des contrats (PSC), Travaux publics et Services gouvernementaux Canada (TPSGC).

2. Ce contrat comprend un accès à des **marchandises contrôlées.** Avant d'avoir accès, le soumissionnaire doit être inscrit au Programme des Marchandises Contrôlées de **Travaux publics et Services gouvernementaux Canada (TPSGC).**

3. Les membres du personnel de l'entrepreneur devant avoir accès à des renseignements ou à des biens PROTÉGÉS, ou à des établissements dont l'accès est réglementé, doivent TOUS détenir une cote de FIABILITÉ en vigueur, délivrée ou approuvée par le PSC, TPSGC.

4. L'entrepreneur NE DOIT PAS utiliser leur établissement pour traiter, produire ou entreposer des renseignements ou des biens PROTÉGÉS tant que le PSC, TPSGC ne lui en aura pas donné l'autorisation par écrit.

5. L'entrepreneur NE DOIT PAS utiliser ses propres systèmes informatiques pour traiter, produire ou entreposer électroniquement des renseignements ou des données au niveau PROTÉGÉ tant que le PSC, TPSGC ne lui en aura pas donné l'autorisation par écrit. Lorsque cette autorisation aura été délivrée, ces tâches pourront être exécutées au niveau PROTÉGÉ B.

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

7. L'entrepreneur doit se conformer aux dispositions des documents suivants :

   a) de la Liste de vérification des exigences relatives à la sécurité et directive de sécurité (s'il y a lieu), reproduite ci-joint à l'Annexe D2;
   b) du *Manuel de la sécurité des contrats* (dernière édition).