MODIFICATION NO. 1

Supprimer l'Annexe C – Liste de Vérification des Exigences Relatives à la Sécurité (LVERS) et Exigences en matière de la sécurité de la TI

Remplacer par :

ANNEX C – EXIGENCES RELATIVES À LA SECURITÉ ET EXIGENCES EN MATIÈRE DE LA SÉCURITÉ EN TI

Government of Canada / Gouvernement du Canada

RECEIVED OCT 05 2017

Contract Number / Numéro du contrat
1000184378Amended
Security Classification / Classification de sécurité UNCLASSIFIED

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

PART A - CONTRACT INFORMATION / PARTIE A - INFORMATION CONTRACTUELLE

1. Originating Government Department or Organization / Ministère ou organisme gouvernemental d'origine	2. Branch or Directorate / Direction générale ou Direction
Aboriginal Affairs and Northern Development Canada	TAG-NW
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

Provide specialized legal translation services from English to French and French to English

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
1000184378Amended
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?

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?

Government of Canada / Gouvernement du Canada

Contract Number / Numéro du contrat
1000184378Amended
Security Classification / Classification de sécurité UNCLASSIFIED

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

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

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

SUMMARY CHART / TABLEAU RÉCAPITULATIF

Category Catégorie	PROTECTED PROTÉGÉ			CLASSIFIED CLASSIFIÉ			NATO				COMSEC					
	A	B	C	CONFIDENTIAL CONFIDENTIEL	SECRET	TOP SECRET TRÈS SECRET	NATO RESTRICTED NATO DIFFUSION RESTREINTE	NATO CONFIDENTIAL NATO CONFIDENTIEL	NATO SECRET	COSMIC TOP SECRET COSMIC TRÈS SECRET	PROTECTED PROTÉGÉ A	 B	 C	CONFIDENTIAL CONFIDENTIEL	SECRET	TOP SECRET TRÈS 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).

Indigenous and Northern Affairs Canada | Affaires autochtones et du Nord Canada

Exigences en matière de sécurité de la TI

Nom entrepreneur	**RFP**
Numéro de contrat :	**1000184378**
Numéro de document :	**9864711**
Numéro de version du document:	**1**
Date:	**2017-01-05**
Designation:	**UNCLASSIFIED**

Aperçu

Conformément à la liste de vérification des exigences relatives à la sécurité (LVERS) pour le contrat n° 1000184378, le fournisseur peut consulter, stocker et transmettre des renseignements classés au niveau Protégé B. Le fournisseur doit veiller à ce que ces renseignements soient protégés en tout temps, conformément à la Politique

sur la sécurité du gouvernement (PSG) (http://www.tbs-sct.gc.ca/pol/doc-fra.aspx?section=text&id=16578) du Conseil du Trésor, à la Norme opérationnelle de sécurité : Gestion de la sécurité des technologies de l'information (GSTI) (http://www.tbs-sct.gc.ca/pol/doc-fra.aspx?id=12328&section=text) du Conseil du Trésor et aux exigences relatives à la sécurité de l'information Affaires autochtones et du Nord Canada (AANC) énoncées dans le présent document.

Services publics et Approvisionnement Canada (SPAC) pourrait procéder à des inspections sur place afin de vérifier et d'attester que le fournisseur satisfait à ces exigences. Il prendra note des éléments non conformes et en avisera le fournisseur et AANC afin que des mesures soient prises immédiatement.

Le fournisseur recevra une copie du présent document. Il connaîtra donc ces exigences en matière de sécurité et saura qu'il doit:

- s'y conformer;
- signaler immédiatement la perte ou le vol de tout dispositif qui renferme des données d'AANC à l'agent de sécurité du Ministère;
- aviser l'agent de sécurité du Ministère de toute infraction réelle ou potentielle à la sécurité qui pourrait avoir une incidence sur les données d'AANC;
- communiquer ces exigences à tout le personnel qui traitera les données d'AANC.

Le non-respect de ces exigences constitue une violation des obligations contractuelles et pourrait entraîner la résiliation du contrat.

Possession, transport et traitement des données ministérielles électroniques

Lorsqu'il transporte, traite ou stocke électroniquement des renseignements ministériels, le fournisseur doit protéger les données en tout temps, peu importe le niveau de confidentialité de l'information, en respectant les exigences suivantes:

- Les systèmes informatiques utilisés pour traiter les données d'AANC sont dotés d'un logiciel antivirus à jour qui est configuré pour recevoir et installer automatiquement les mises à niveau de produits.
- Les systèmes informatiques utilisés pour traiter les données d'AANC sont dotés de versions de logiciels et de systèmes d'exploitation à jour qui sont configurés pour recevoir et installer automatiquement les mises à niveau.
- Les systèmes informatiques sont protégés par un pare-feu; il peut s'agir d'un mécanisme de pare-feu du périmètre du réseau ou d'un pare-feu installé sur l'ordinateur (remarque : un pare-feu ne peut pas être remplacé uniquement par un routeur standard).
- Le fournisseur est en mesure de disposer des données électroniques de manière sécuritaire, conformément aux normes du Centre de la sécurité des télécommunications Canada (consulter le site hhttps://www.cse-cst.gc.ca/fr/node/270/html/10572).
- Les données ministérielles doivent être stockées sur un support amovible certifié de type FIPS 140-2 ou supérieur, chiffré avec un algorithme AES de 128 bits ou davantage (consulter le site http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/1401vend.htm pour la liste des appareils certifiés);
- Les supports de stockage portatifs doivent être étiquetés pour indiquer le plus haut niveau de classification ou de désignation de l'information qui y est stockée.

Stockage physique des données ministérielles

S'il stocke des données ministérielles électroniques dans ses locaux, le fournisseur doit protéger les données lorsqu'elles ne sont pas utilisées en respectant les exigences suivantes:

- Les supports amovibles chiffrés doivent être entreposés dans un coffre de sécurité approprié, en fonction du niveau de classification le plus élevé de l'information qu'ils contiennent. Le fournisseur doit posséder un tel coffre de sécurité dans ses locaux (Protégé A ou B = coffre de sécurité à cadenas / Protégé C et Secret = coffre de sécurité avec serrure à combinaisons intégrée – consulter le site http://www.rcmp-grc.gc.ca/ts-st/reslim/pubs/seg/html/home_f.htm pour de plus amples renseignements).

Transmission électronique de données ministérielles

Lorsqu'il transmet des données ministérielles par voie électronique à AANC, le fournisseur doit s'assurer de n'utiliser que les méthodes approuvées, selon le niveau de sensibilité de l'information. Le fournisseur peut faire appel à une combinaison de ces modes de transmission pour échanger des renseignements avec le personnel d'AANC. L'utilisation de modes de transmission électronique autres que ceux énumérés ci-dessous est interdite.

Note : Le ministère a certifié et accrédité son service de connectivité à distance pour l'accès à et/ou la transmission d'information jusqu'à protégée B. AANC accepte les risques résiduels d'utilités pour la période du contrat. Une inspection TI par SPAC de vérifier l'accès à distance n'est donc pas requise.

Niveau de classification	Mode de transmission approuvé par AANC	Exigences
Protégé A	Courriel	Le fournisseur peut transmettre des données Protégé A par courriel au personnel d'AANC pourvu qu'il respecte les exigences suivantes : • Le compte courriel n'est pas un service de messagerie accessible au public sur le Web (p. ex. Hotmail, Yahoo, Gmail, etc.). • Chaque utilisateur a son propre compte courriel d'entreprise protégé par un nom d'utilisateur et un mot de passe. • Les communications entre les serveurs de courriel sont protégées par le chiffrement TLS.
	Télécopieur	Le fournisseur peut transmettre des données Protégé A par télécopieur à AANC pourvu qu'il respecte les exigences suivantes : • Le télécopieur se trouve dans les locaux du fournisseur. • L'expéditeur téléphone d'abord au destinataire pour l'informer de l'envoi à venir et confirmer le numéro de télécopieur. • Le destinataire est à côté du télécopieur, prêt à recevoir l'envoi. • L'expéditeur obtient une confirmation de réception.
	Communications sans fil	Si un point d'accès sans fil est installé dans les locaux de l'entrepreneur, et que les dispositifs de traitement des données d'AANC seront connectés à ce réseau, l'infrastructure sans fil doit au minimum inclure les mesures de protection suivantes : ▪ Le nom et le mot de passe de l'administrateur par défaut doivent être changés.

		▪ Le nom du réseau (SSID) par défaut a été changé. ▪ Le chiffrage WPA2 avec l'algorithme AES est activé et la phrase passe répond aux exigences de complexité suivantes : • comporter au moins 8 caractères; • contenir au moins une lettre majuscule; • contenir au moins une lettre minuscule; • contenir au moins un chiffre; • contenir au moins un caractère spécial.
Protégé B	Courriel chiffré et portant une signature numérique	Le fournisseur peut transmettre des données Protégé B au personnel d'AANC par courriel pourvu que les messages et/ou les pièces jointes soient chiffrés et qu'il respecte les exigences suivantes : • Le compte courriel n'est pas un service de messagerie accessible au public sur le Web (p. ex. Hotmail, Yahoo, Gmail, etc.). • Chaque utilisateur a son propre compte courriel d'entreprise protégé par un nom d'utilisateur et un mot de passe. • Le fournisseur a un certificat d'infrastructure à clé publique (ICP) approuvé, qui est compatible avec les services d'ICP du gouvernement du Canada (GC). • Le logiciel Entrust est installé sur l'ordinateur de bureau ou l'ordinateur portable du fournisseur et sert à chiffrer les courriels en appliquant les paramètres suivants : • L'un des algorithmes de chiffrement suivants est utilisé **:** ▪ 3DES-168 bits ou davantage ▪ AES-128 bits ou davantage • Les courriels sont signés numériquement à l'aide de l'un des algorithmes suivants : ▪ RSA (algorithme de Rivest-Shamir-Adleman) ▪ ASN (algorithme de signature numérique) ▪ ASNCE (algorithme de signature numérique à courbe elliptique) • L'un des algorithmes de hachage suivants sert à générer les signatures numériques : • SHA-224 • SHA-256 • SHA-384 • SHA-512

	Communications sans fil	Si un point d'accès sans fil est installé dans les locaux de l'entrepreneur, et que les dispositifs de traitement des données d'AANC seront connectés à ce réseau, l'infrastructure sans fil doit au minimum inclure les mesures de protection suivantes : ▪ Le nom et le mot de passe de l'administrateur par défaut doivent être changés. ▪ Le nom du réseau (SSID) par défaut a été changé. ▪ Le chiffrage WPA2 avec l'algorithme AES est activé et la phrase passe répond aux exigences de complexité suivantes : • comporter au moins 12 caractères; • contenir au moins une lettre majuscule; • contenir au moins une lettre minuscule; • contenir au moins un chiffre; • contenir au moins un caractère spécial.
	Service de transfert sécurisé des fichiers d'AANC	Le fournisseur peut transmettre des données Protégé B par le biais du service de transfert sécurisé des fichiers d'AANC pourvu qu'il respecte les exigences suivantes : • Un nom d'utilisateur et un mot de passe personnels et uniques sont assignés à chaque utilisateur par AANC. • Le fournisseur a lu la Politique sur l'utilisation acceptable : Service de transfert sécurisé des fichiers d'AANC (https://efse-sfee.AANC-aandc.gc.ca/politique/efs_politique_utilisation_acceptable.html) et s'engage à la respecter.
	Service Collaboration d'AANC	Le fournisseur peut transmettre des données Protégé B par le biais du service Collaboration d'AANC pourvu qu'il respecte les exigences suivantes : • Un nom d'utilisateur et un mot de passe personnels et uniques sont assignés à chaque utilisateur par AANC.
	Télécopieur	Le fournisseur peut transmettre des données Protégé B par télécopieur à AANC pourvu qu'il respecte les exigences suivantes : • Le télécopieur se trouve dans les locaux du fournisseur. • L'expéditeur téléphone d'abord au destinataire pour l'informer de l'envoi à venir et confirmer le numéro de télécopieur. • Le destinataire est à côté du télécopieur, prêt à recevoir l'envoi. • L'expéditeur obtient une confirmation de réception.