Annexe A
Appendice 1 — Obligations en matière de sécurité
pour SaaS de palier 2 (jusqu'au niveau Protégé B inclusivement)

1. Généralités

1.1 Objet

Le présent appendice a pour objet d'énoncer les obligations de l'entrepreneur en matière de bonne gestion des données du Canada, y compris la protection contre les modifications, les exfiltrations et les accès non autorisés, conformément à l'entente, au présent appendice et aux mesures de sécurité de l'entrepreneur (collectivement, les « **obligations en matière de sécurité** »).

1.2 Transfert des obligations en matière de sécurité

Les obligations de l'entrepreneur contenues dans les présentes obligations en matière de sécurité doivent être transférées par l'entrepreneur à ses sous-traitants dans la mesure où elles s'appliquent à ces derniers.

1.3 Gestion des changements

L'entrepreneur doit, pendant toute la durée du contrat, prendre toutes les mesures nécessaires pour mettre à jour et maintenir les obligations en matière de sécurité afin de se conformer aux pratiques de sécurité des normes de l'industrie énoncées dans le présent appendice.

L'entrepreneur doit informer le Canada de tous les changements qui nuisent ou qui pourraient nuire sensiblement aux services infonuagiques offerts dans le cadre du présent contrat, y compris les changements ou les améliorations de nature technologique, administrative ou autre. L'entrepreneur accepte d'offrir toutes les améliorations qu'il offre à ses clients en général dans le cadre de son service régulier, sans supplément pour le Canada.

2. Reconnaissance

Les parties reconnaissent ce qui suit :

(a) Les données du Canada sont assujetties aux présentes obligations en matière de sécurité.

(b) Nonobstant toute autre disposition du présent appendice, les parties partagent la responsabilité de l'élaboration et du maintien des politiques, des procédures et des contrôles de sécurité relatifs aux données du Canada.

(c) L'entrepreneur ne doit pas avoir en sa possession ou tenter d'avoir en sa possession des données du Canada, ni permettre à aucun membre du personnel des services infonuagiques d'y avoir accès avant que ne soient instaurées les obligations en matière de sécurité prévues au présent appendice, au plus tard à la date d'attribution du contrat.

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

3. Protection des données du Canada

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

4. Rôles et responsabilités liés à la sécurité

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

(2) L'entrepreneur doit fournir au Canada un document à jour qui définit les rôles et les responsabilités : i) au moment de l'attribution du contrat; ii) chaque année; iii) lorsque des changements importants sont apportés à ces rôles et responsabilités à la suite d'une modification des services infonuagiques; ou iv) à la demande du Canada.

5. Assurance d'une tierce partie : certifications et rapports

(1) L'entrepreneur doit veiller à ce que les données du Canada, l'infrastructure de l'entrepreneur (y compris les services IaaS, PaaS ou SaaS fournis au Canada) et les points de prestation des services soient protégés par des mesures de sécurité appropriées qui sont conformes aux exigences énoncées dans ses pratiques et politiques de sécurité.

(2) L'entrepreneur doit démontrer que les mesures sont conformes aux exigences énoncées dans les certifications suivantes en fournissant des rapports d'évaluation ou des certifications de tiers indépendants qui portent sur chaque couche de service (p. ex. IaaS, PaaS et SaaS) au sein de l'offre de services infonuagiques, notamment :

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

(b) ISO/IEC 27017:2015 Technologies de l'information —

Techniques de sécurité — Code de pratique pour les contrôles de sécurité de l'information fondés sur la norme ISO/IEC 27002 pour les services infonuagiques, obtenue par un organisme de certification accrédité; ET

(c) Contrôles au niveau du système et au niveau organisationnel de l'AICPA (Service Organization Control) (SOC) 2 Type I — Rapport de vérification 2 de type II se rapportant aux principes des services Trust (sécurité, disponibilité, intégrité du traitement et confidentialité) — produit par un comptable public accrédité (CPA) indépendant..

(3) Chaque rapport de certification ou de vérification fourni doit : i) mentionner le nom légal de l'entreprise de l'entrepreneur ou du sous-traitant applicable; ii) mentionner la date de certification de l'entrepreneur ou du sous-traitant et l'état de cette certification; et iii) dresser la liste des services visés par le rapport de certification. Si des exclusions sont relevées, ou s'il est nécessaire de séparer des services de sous-traitants comme l'hébergement de centres de données, le rapport d'évaluation du sous-traitant doit être inclus.

(4) Chaque vérification doit faire l'objet d'un rapport qui sera mis à la disposition du Canada. Les certifications doivent être accompagnées d'éléments de preuve à l'appui, comme le rapport d'évaluation ISO élaboré pour valider la conformité avec la certification ISO, et elles doivent clairement divulguer toutes les constatations importantes du vérificateur. L'entrepreneur doit régler rapidement tout problème soulevé dans un rapport de vérification, à la satisfaction du vérificateur.

(5) Chaque rapport SOC 2 type II doit avoir été réalisé dans les 12 mois précédant le début du contrat. Une lettre de transition peut être fournie pour démontrer que l'entrepreneur attend son renouvellement, s'il y a un écart entre la date du rapport du fournisseur de services et la fin de l'exercice de l'organisation utilisatrice (année civile ou fiscale)

(6) L'entrepreneur doit conserver les certifications ISO 27001, ISO 27017 et SOC 2 Type II pour toute la durée du contrat. L'entrepreneur doit fournir, au moins une fois par année et rapidement à la demande du Canada, tous les rapports ou documents pouvant être raisonnablement exigés pour démontrer que l'entrepreneur possède des certifications actuelles.

6. Vérification de la conformité

(1) L'entrepreneur doit effectuer les vérifications de confidentialité et de sécurité portant sur la sécurité des ordinateurs, l'environnement informatique et les centres de données physiques qu'il utilise pour traiter et protéger les données du Canada, de la manière suivante :

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

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

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

(2) Chaque vérification donnera lieu à la production d'un rapport de vérification qui doit être mis à la disposition du Canada. Le rapport de vérification doit indiquer clairement toutes les constatations importantes faites par le tiers vérificateur. L'entrepreneur doit, à ses frais, corriger rapidement et à la satisfaction du vérificateur les problèmes et les lacunes soulevés dans tout rapport de vérification.

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

7. Programme d'évaluation de la sécurité des TI du fournisseur de services infonuagiques (FSI)

(1) L'entrepreneur doit démontrer qu'il respecte les exigences en matière de sécurité sélectionnées dans le Profil des mesures de sécurité pour les services du GC fondés sur l'informatique en nuage pour les renseignements classés PROTÉGÉ B, intégrité moyenne, disponibilité moyenne (PBMM) (https://www.canada.ca/fr/gouvernement/systeme/gouvernement-numerique/innovations-gouvernementales-numeriques/services-informatique-nuage/profil-controle-securite-services-ti-fondes-information-nuage.html, selon la portée des services infonuagiques fournis par l'entrepreneur. La conformité doit être démontrée par la mise en correspondance des contrôles de sécurité avec les certifications de l'industrie applicables énoncées ci-dessous, puis validée au moyen d'évaluations de tiers indépendants.

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

L'entrepreneur doit démontrer qu'il a participé au processus en réussissant l'intégration, la réalisation et l'achèvement du programme. Entre autres, il lui faudra produire les documents suivants :

(i) Une copie de la lettre de confirmation qui indique qu'il a adhéré au programme;
(ii) Une copie du dernier rapport d'évaluation rempli fourni par le CCC;
(iii) Une copie du dernier rapport sommaire fourni par le CCC.

L'entrepreneur qui souhaite en savoir plus sur le processus d'évaluation STI du CCC visant les FSI doit communiquer avec le service à la clientèle du CCC.

En tout temps, il incombe à l'entrepreneur des services infonuagiques proposés d'avertir le CCC lorsque des changements importants sont apportés à la prestation des services de sécurité des TI associée à son offre.

La conformité doit être démontrée par la mise en correspondance des contrôles de sécurité avec les certifications de l'industrie applicables énoncées ci-dessous, puis validée au moyen d'évaluations de tiers indépendants.

(3) Dans le cas où l'entrepreneur est un fournisseur d'IaaS approuvé par le gouvernement du Canada qui se conforme déjà aux dispositions de la section 5 — Assurance de tierce partie et des paragraphes (1) et (2) de la section 7 — Programme d'évaluation de la sécurité des TI du fournisseur de services infonuagiques (FSI), le fournisseur de SaaS doit présenter au Canada une copie d'un courriel envoyé par le Centre canadien pour la cybersécurité (CCC) confirmant que le soumissionnaire a terminé le processus d'évaluation STI du CCC visant les FSI. Le courriel doit préciser que le FSI a été évalué par le processus d'évaluation STI du CCC visant les FSI et qu'il a reçu un rapport final concernant l'évaluation. Vous pouvez envoyer vos questions par courriel au CCC à l'adresse contact@cyber.gc.ca.

8. Protection des données

(1) L'entrepreneur doit :

(a) Mettre en œuvre le chiffrement des données inactives pour tous les services infonuagiques qui hébergent des données du Canada lorsque le chiffrement des données inactives demeure en vigueur, ininterrompu et actif en tout temps, même en cas de panne d'équipement ou de technologie, conformément à la section 13 — Protection cryptographique;

(b) Transmettre les données du Canada de façon sécuritaire, y compris la capacité, pour le GC, de mettre en œuvre le chiffrement des données en cours de transfert pour toutes les transmissions de données du Canada, conformément à la section 13 — Protection cryptographique et à la section 21 — Sécurité des réseaux et des communications;

(c) Mettre en place des contrôles de sécurité qui restreignent l'accès administratif aux données et aux systèmes du Canada par l'entrepreneur et qui permettent d'exiger l'approbation du gouvernement du Canada avant que l'entrepreneur puisse accéder aux données du Canada pour effectuer des activités de soutien, d'entretien ou d'exploitation;

(d) Prendre des mesures raisonnables pour s'assurer que le personnel de l'entrepreneur n'a pas de droits d'accès permanents ou continuels aux données du Canada, et que l'accès est limité au personnel de l'entrepreneur ayant un besoin de savoir, y compris les ressources qui fournissent un soutien technique ou à la clientèle, en fonction de l'approbation du gouvernement du Canada.

(2) L'entrepreneur ne doit pas faire de copies des bases de données ou de parties de ces bases de données contenant des données du Canada à l'extérieur des capacités de résilience des services réguliers et dans les lieux ou zones régionaux approuvés au Canada.

(3) L'entrepreneur doit s'assurer que tout traitement effectué hors du Canada, y compris le déplacement ou la transmission de copies approuvées des données, a lieu dans les régions de service convenues.

(4) À la demande du Canada, l'entrepreneur doit fournir au Canada un document décrivant toutes les métadonnées supplémentaires créées à partir des données du Canada.

9. Isolement des données

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

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

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

(c) La capacité du GC de prendre en charge l'isolement dans un environnement à locataires géré par le GC.

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

10. Emplacement des données

(1) L'entrepreneur doit stocker et protéger les données du Canada inactives, y compris les données sauvegardées ou conservées aux fins de redondance. Cela comprend la capacité d'isoler les données au Canada dans des centres de données approuvés. Un centre de données approuvé possède les caractéristiques suivantes :

(a) Il répond à toutes les exigences et certifications de sécurité exposées dans la section 30 concernant la sécurité physique (centre de données/installations);

(b) Il garantit l'impossibilité de trouver les données d'un client en particulier sur des supports physiques;

(c) Il emploie le chiffrement pour s'assurer qu'aucune donnée n'est écrite sur disque sous une forme non chiffrée, conformément à la section 13 — Protection cryptographique.

(2) L'entrepreneur doit certifier que la prestation et l'approvisionnement des services infonuagiques en vertu du présent contrat proviennent de pays de l'Organisation du Traité de l'Atlantique Nord (OTAN) (https://www.nato.int/cps/fr/natohq/index.htm), de pays européens

(UE) (https://europa.eu/european-union/about-eu/countries_en), ou des pays avec lesquels le Canada dispose d'un dispositif bilatéral de sécurité industrielle internationale. Dans le cadre du Programme de sécurité des contrats (PSC), des accords internationaux bilatéraux en matière de sécurité industrielle ont été conclus avec les pays indiqués sur le site Web https://www.tpsgc-pwgsc.gc.ca/esc-src/international-fra.html du PSC, mis à jour ponctuellement.

(3) L'entrepreneur doit mettre en œuvre la capacité pour le Canada d'isoler les données du Canada hébergées dans des services infonuagiques dans des centres de données géographiquement situés au Canada.

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

(a) Fournir au GC une liste à jour des emplacements physiques, y compris la ville, pouvant stocker les données du Canada inactives;

(b) Indiquer les parties des services infonuagiques qui sont fournies depuis l'étranger, y compris tous les endroits où les données sont stockées et traitées et d'où l'entrepreneur gère le service.

(5) L'entrepreneur des services infonuagiques proposés a l'obligation permanente d'avertir le Canada lorsque des mises à jour sont apportées à la liste des emplacements physiques où peuvent se trouver les données du Canada inactives.

11. Transfert et récupération des données

L'entrepreneur doit fournir au Canada la capacité suivante, notamment des outils et des services :

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

(b) Effectuer le transfert sécurisé de toutes les données du Canada, y compris les données de contenu et les métadonnées connexes, dans un format lisible et utilisable par machine (y compris le format CSV) et conformément aux *Lignes directrices sur les formats de fichier à utiliser pour transférer des ressources documentaires à valeur continue* de Bibliothèque et Archives Canada (https://www.bac-lac.gc.ca/fra/services/gestion-ressources-documentaires-gouvernement/lignes-directrices/Pages/lignes-directrices-formats-fichier-

transferers-ressources-documentaires.aspx).

12. Élimination des données et remise des documents au Canada

(1) L'entrepreneur doit éliminer ou réutiliser en toute sécurité les ressources (p. ex. l'équipement, le stockage des données, les fichiers et la mémoire) qui contiennent des données du Canada et s'assurer que les données précédemment stockées ne peuvent pas être traitées par d'autres clients après leur diffusion. Cette mesure concerne toutes les copies des données du Canada qui sont créées à des fins de disponibilité accrue et de reprise après sinistre. L'élimination ou la réutilisation des ressources par l'entrepreneur doit être harmonisée à l'une des pratiques exemplaires suivantes :

(i) *National Industrial Security Program Operating Manual* (DoD 5220.22-M6); ii) *Guidelines for Media Sanitization* (NIST SP 800-88); ou iii) *Effacement et déclassification des supports d'information électroniques* (CST ITSG-06). À la demande du Canada, l'entrepreneur doit produire un document qui décrit son processus d'élimination ou de réutilisation des ressources.

(2) L'entrepreneur doit présenter au Canada la confirmation démontrant qu'il a réussi à effacer, à purger ou à détruire toutes les ressources, selon le cas, et qu'il est en mesure d'empêcher le rétablissement de tout système, de toute capacité (logiciel ou processus), de toute donnée ou de toute information retirés ou détruits une fois que le Canada a cessé d'utiliser les services infonuagiques.

13. Protection cryptographique

L'entrepreneur doit :

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

(b) Utiliser des algorithmes cryptographiques, des tailles de clés de chiffrement et des périodes de validité des clés validés par le Cryptographic Algorithm Validation Program (http://csrc.nist.gov/groups/STM/cavp/, en anglais seulement), et précisés dans le document ITSP.40.111 *Algorithmes cryptographiques pour l'information NON CLASSIFIÉ, PROTÉGÉ A et PROTÉGÉ B* ou dans des versions subséquentes de ce document (https://cyber.gc.ca/fr/orientation/algorithmes-cryptographiques-pour-linformation-non-classifie-protege-et-protege-b);

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

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

14. Gestion des clés

L’entrepreneur doit s’assurer qu’un service de gestion des clés peut être utilisé, avec les capacités suivantes, entre autres :

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

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

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

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

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

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

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

15. Protection des points terminaux

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

16. Développement sécurisé

L’entrepreneur doit mettre en œuvre un cycle de vie de développement de logiciels et de systèmes qui applique les principes d’ingénierie de la sécurité des systèmes d’information tout au long de leur cycle de vie et dans le développement de logiciels, de sites Web et de services. Ce cycle de vie doit être conforme aux normes et aux pratiques exemplaires du secteur, comme : i) NIST, ii) ISO 27034, iii) ITSG-33, iv) SAFECode ou v) Open Web Application Security Project (OWASP) (p. ex. Application Security Verification Standard [ASVS]) ou une norme équivalente approuvée par le Canada par écrit. À la demande du Canada, l’entrepreneur doit produire un document qui décrit le logiciel documenté de l’entrepreneur, ainsi que l’approche et le processus adoptés relativement au cycle de vie du développement du système.

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

(1) L'entrepreneur doit mettre en œuvre la capacité pour le Canada de prendre en charge un accès sécurisé aux services infonuagiques, y compris la capacité de configurer :

(a) L'authentification multifactorielle conformément à l'ITSP.30.031 V3 du CST (ou versions ultérieures) (https://cyber.gc.ca/fr/orientation/guide-sur-lauthentification-des-utilisateurs-dans-les-systemes-de-technologie-de) à l'aide d'identifiants approuvés par le gouvernement du Canada;

(b) Un accès basé sur les rôles;

(c) Des contrôles de l'accès aux objets stockés;

(d) Des politiques d'autorisation granulaire pour autoriser ou limiter l'accès.

(2) L'entrepreneur doit avoir la capacité d'établir des paramètres par défaut à l'échelle de l'organisation pour gérer les politiques applicables à l'ensemble des locataires.

18. Fédération

(1) L'entrepreneur doit mettre en œuvre la capacité pour le Canada de prendre en charge l'intégration fédérée de l'identité, y compris :

(a) Prendre en charge des normes ouvertes pour les protocoles d'authentification comme le langage SAML (Security Assertion Markup Language) 2.0 ou OpenID Connect 1.0 (ou versions ultérieures), selon lesquels les identifiants de l'utilisateur final et l'authentification aux services infonuagiques relèvent exclusivement du Canada;

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

19. Gestion de l'accès privilégié

(1) L'entrepreneur doit :

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

(b) Restreindre et réduire au minimum l'accès aux services infonuagiques et aux données du Canada seulement aux appareils autorisés et aux utilisateurs finaux ayant explicitement besoin de cet accès;

(c) Appliquer et vérifier les autorisations d'accès aux services infonuagiques et aux données du Canada;

(d) Limiter tous les accès aux interfaces de service qui hébergent les données du Canada à des utilisateurs finaux, des dispositifs et des processus (ou des services) identifiés, authentifiés et autorisés de manière unique;

(e) Mettre en œuvre des politiques sur les mots de passe afin de protéger les identifiants contre les attaques en ligne ou hors ligne et de détecter ces attaques en consignant et en surveillant des événements tels que i) l'utilisation réussie des identifiants, ii) l'utilisation inhabituelle de ces derniers et iii) l'accès et l'exfiltration des mots de passe depuis la base de données, conformément à la version 3 (ou aux versions ultérieures) de la norme ITSP.30.031 du CST (https://cyber.gc.ca/fr/orientation/guide-sur-lauthentification-des-utilisateurs-dans-les-systemes-de-technologie-de);

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

(g) Mettre en œuvre des mécanismes d'authentification multifactorielle pour authentifier les utilisateurs finaux ayant un accès privilégié, conformément à la norme ITSP.30.031 V3 (ou versions ultérieures) du CST (https://cyber.gc.ca/en/guidance/user-authentication-guidance-information-technology-systems-itsp30031-v3);

(h) Mettre en place des mécanismes de contrôle de l'accès fondés sur le rôle qui forment la base de l'accès aux données du Canada;

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

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

(k) Utiliser des terminaux à sécurité renforcée (p. ex. ordinateurs, dispositifs d'utilisateurs finaux, serveurs intermédiaires) configurés de façon à offrir une fonctionnalité minimale (p. ex. terminal spécialisé qui ne peut pas être utilisé pour naviguer sur Internet ou consulter ses courriels) afin d'assurer la prise en charge et l'administration des services infonuagiques et de l'infrastructure de l'entrepreneur;

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

(m) Révoquer, en cas de cessation d'emploi, les authentifiants et les identifiants d'accès associés à tout membre du personnel de services.

(2) À la demande du Canada, l'entrepreneur doit produire un document qui décrit l'approche et le processus de l'entrepreneur pour la gestion et la surveillance des accès privilégiés aux services infonuagiques.

20. Gestion à distance

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

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

(b) Employer des mécanismes et des algorithmes cryptographiques pour protéger la confidentialité des séances d'accès à distance, conformément à la section 13 — Protection cryptographique;

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

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

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

(2) À la demande du Canada, l'entrepreneur doit produire un document qui décrit l'approche et le processus de l'entrepreneur pour la gestion et la surveillance de l'administration à distance des services infonuagiques.

21. Sécurité des réseaux et des communications

L'entrepreneur doit :

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

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

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

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

22. Accès et vérification

(1) L'entrepreneur doit mettre en œuvre des pratiques et des contrôles de création et de gestion des journaux pour toutes les composantes des services infonuagiques qui stockent ou traitent les données du Canada, et qui sont conformes aux normes et aux pratiques exemplaires de l'industrie, comme celles énoncées dans le document NIST 800-92 - *Guide to computer Security Log Management* ou une norme équivalente approuvée par écrit par le Canada. À la demande du Canada, l'entrepreneur doit produire un document décrivant ses pratiques et contrôles de création et de gestion des journaux.

(2) L'entrepreneur doit donner au Canada les capacités d'exporter des journaux des événements de sécurité à l'aide d'interfaces de rapport, de protocoles et de formats de données normalisés (p. ex. Common Event Format [CEF], journal d'exploitation ou autres formats de journal communs) et d'API qui prennent en charge l'extraction à distance des données des journaux (p. ex. au moyen d'une interface de base de données utilisant SQL), pour les services infonuagiques qu'il utilise, pour appuyer les activités du GC, y compris la surveillance des services infonuagiques et la divulgation électronique et les mises en suspens pour des raisons juridiques.

(3) L'entrepreneur doit permettre au Canada d'examiner et d'analyser de façon centralisée les dossiers de vérification de multiples composantes des services infonuagiques utilisés par le client. Entre autres, il lui faudra fournir des API qui permettent d'inspecter et d'interroger les données inactives dans les applications SaaS, y compris par l'évaluation d'événements comme l'accès et le comportement des utilisateurs, l'accès et le comportement des administrateurs et les changements apportés à l'accès aux API de tiers stockées dans les registres d'applications SaaS.

23. Surveillance continue

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

(a) Surveiller activement et continuellement les menaces et les vulnérabilités pesant sur l'infrastructure de l'entrepreneur, les points de prestation des services ou les données du Canada;

(b) Tout mettre en œuvre pour prévenir les attaques au moyen de mesures de sécurité comme les protections contre le déni de service;

(c) Tout mettre en œuvre pour détecter les attaques, les incidents de sécurité et autres événements anormaux;

(d) Détecter l'utilisation et l'accès non autorisés à tous les services infonuagiques, données et composants afférents aux services infonuagiques IaaS, PaaS ou SaaS

du Canada;

(e) Gérer et appliquer les correctifs et les mises à jour liés à la sécurité de manière opportune et systématique afin d'atténuer les vulnérabilités et de corriger tout problème signalé publiquement dans les services infonuagiques ou les bibliothèques que les services infonuagiques utilisent, et donner des préavis de correctif conformément aux engagements convenus relatifs au niveau de service;

(f) Répondre aux menaces et aux attaques contre les services infonuagiques de l'entrepreneur, les contenir et veiller à la récupération;

(g) Au besoin, prendre des contre-mesures proactives, y compris des mesures préventives et d'intervention permettant d'atténuer les menaces.

(2) Les services infonuagiques publics de l'entrepreneur doivent permettre de copier les données des applications des services du GC hébergés en nuage et de les acheminer vers un emplacement prédéterminé (dans le nuage ou dans les locaux du GC).

24. Gestion des incidents de sécurité

(1) Le processus d'intervention de l'entrepreneur en cas d'incident de sécurité pour les services infonuagiques doit englober le cycle de vie de la gestion des incidents de sécurité des TI et les pratiques de prise en charge des activités de préparation, de détection, d'analyse, de confinement et de reprise. Cela comprend ce qui suit :

(a) Un processus d'intervention en cas d'incident de sécurité publié et documenté en vue de l'examen par le Canada, conforme à l'une des normes suivantes : i) ISO/IEC 27035:2011 *Information technology — Security techniques — Information security incident management*; ii) NIST SP800-612, *Computer Security Incident Handling Guide*; iii) *Plan de gestion des événements de cybersécurité du gouvernement du Canada* (PGEC GC) (https://www.canada.ca/fr/gouvernement/systeme/gouvernement-numerique/securite-confidentialite-ligne/gestion-securite-identite/plan-gestion-evenements-cybersecurite-gouvernement-canada.html); iv) d'autres pratiques exemplaires tirées des normes de l'industrie, si le Canada détermine, à sa discrétion, qu'elles satisfont aux exigences canadiennes en matière de sécurité;

(b) Des processus et des procédures documentés sur la façon dont l'entrepreneur détectera les incidents de sécurité de l'information, y donnera suite, les corrigera, les signalera et en fera part au Canada, notamment :
(i) La portée des incidents liés à la sécurité de l'information que l'entrepreneur signalera au Canada; ii) le niveau de divulgation de la détection des incidents liés à la sécurité de l'information et les interventions connexes; iii) le délai cible de notification des incidents liés à la sécurité de l'information; iv) la procédure de notification des incidents liés à la sécurité de l'information; v) les coordonnées des personnes-ressources pour le traitement des problèmes liés aux incidents liés à la sécurité de l'information et vi) tous les recours qui s'appliquent si certaines mesures de sécurité de l'information sont prises.

(c) La capacité de l'entrepreneur d'appuyer les efforts d'enquête du Canada en cas de constat de compromission des utilisateurs ou des données du service;

(d) Autorise uniquement les représentants du client (comme le Centre des opérations de sécurité de SPC) désignés par le responsable technique :

(i) À demander et à recevoir un accès et de l'information confidentiels associés aux données du client (données des utilisateurs, journaux d'événements du système et de sécurité, saisies de paquets du réseau ou de l'hôte, journaux de composants de sécurité comme des systèmes de détection et de prévention d'intrusion et des pare-feu, etc.) dans un format non chiffré, aux fins d'enquête;
(ii) À effectuer le suivi d'un événement signalé lié à la sécurité de l'information;

(e) Des procédures de réponse aux demandes de preuves numériques potentielles ou d'autres renseignements se trouvant dans l'environnement des services infonuagiques, y compris des procédures judiciaires et des mesures de protection pour la tenue d'une chaîne de possession;

(2) À la demande du Canada, l'entrepreneur doit produire un document qui décrit son processus d'intervention en cas d'incident de sécurité.

(3) L'entrepreneur doit :

(a) Travailler avec les centres des opérations de sécurité du Canada (p. ex. le CCC, le COS du ministère) en vue du confinement et de l'élimination de l'incident de sécurité, et de la reprise des activités conformément au processus d'intervention en cas d'incident de sécurité;

(b) Tenir un registre des atteintes à la sécurité comprenant une description de l'atteinte, sa durée, ses conséquences, le nom de la personne qui l'a signalée et celui de la personne à qui elle a été signalée, et la procédure pour récupérer les données ou le service;

(c) Suivre ou permettre au Canada de suivre les divulgations de données du Canada, y compris le type de données divulguées, les personnes y ayant eu accès et le moment où l'incident s'est produit.

(4) Le Canada peut exiger des preuves judiciaires de la part de l'entrepreneur pour faciliter une enquête du GC. L'entrepreneur convient de fournir de l'aide au GC dans la mesure du possible.

25. Intervention en cas d'incident de sécurité

(1) L'entrepreneur doit alerter et informer promptement le Canada (par téléphone ou par courriel) de toute compromission, atteinte à la sécurité ou preuve comme i) un incident de sécurité, ii) une défectuosité liée à la sécurité d'un actif, iii) l'accès irrégulier ou non autorisé à un actif, iv) la copie à grande échelle d'un actif d'information ou v) toute autre activité illégale recensée par l'entrepreneur, portant ce dernier à croire de manière raisonnable que le risque de compromission, d'atteinte à la sécurité ou à la vie privée est ou pourrait être imminent, ou si les mesures de protection existantes ont cessé de fonctionner, au cours de la période suivante (tous les jours, 24 heures par jour, 365 jours par année), et sans tarder, dans tous les cas, dans les 72 heures, et conformément aux engagements convenus relatifs au niveau de service.

(2) Si l'entrepreneur prend connaissance de toute compromission ou atteinte à la sécurité et détermine qu'elle peut entraîner la destruction, la perte, l'altération, la divulgation non autorisée des données ou des données personnelles du client, ou encore l'accès aux données ou aux données personnelles du client, pendant le traitement par l'entrepreneur

(chacun étant un « incident de sécurité »), l'entrepreneur doit rapidement et sans tarder i) informer le Canada de cet incident de sécurité; ii) mener une enquête et fournir au Canada des renseignements détaillés sur cet incident de sécurité; iii) prendre les mesures raisonnables pour remédier aux causes et atténuer les dommages découlant de l'incident de sécurité.

26. Fuite d'information

(1) L'entrepreneur doit disposer d'un processus documenté décrivant son approche en cas d'incident de fuite d'information. Ce processus doit être harmonisé i) aux directives de la section IR-9 intitulée *Intervention en cas de fuite d'information* du document ITSG-33, ou ii) à une autre pratique exemplaire du secteur approuvée par écrit par le Canada. Sans égard à ce qui précède, le processus d'intervention en cas de fuite d'information de l'entrepreneur doit comprendre, à tout le moins :

(a) Un processus d'identification des éléments de données précis utilisés dans la contamination d'un système;

(b) Un processus visant à isoler et à éradiquer un système contaminé;

(c) Un processus d'identification des systèmes pouvant avoir été contaminés par la suite et toute autre mesure prise pour empêcher la propagation de la contamination.

(2) À la demande du Canada, l'entrepreneur doit produire un document qui décrit son processus d'intervention en cas de fuite d'information.

27. Test de sécurité et validation

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

(2) L'entrepreneur doit fournir la capacité d'activer un outil libre-service de vérification de l'état de sécurité ou de notation qui mesure la posture de sécurité des services infonuagiques configurés par le Canada.

28. Filtrage de sécurité du personnel

(1) L'entrepreneur doit mettre en place des mesures de sécurité qui permettent d'accorder et de maintenir le niveau de filtrage de sécurité requis pour le personnel de l'entrepreneur qui participe à la prestation de services infonuagiques et le personnel des sous-traitants en fonction de leurs privilèges d'accès aux actifs des systèmes d'information sur lesquels les données du Canada sont stockées et traitées.

(2) Les mesures de filtrage de l'entrepreneur doivent être appliquées conformément à la définition et aux pratiques énoncées dans la *Norme sur le filtrage de sécurité* du Conseil du Trésor (https://www.tbs-sct.gc.ca/pol/doc-fra.aspx?id=28115), ou utiliser un équivalent acceptable convenu par le Canada.

(3) À la demande du Canada, l'entrepreneur doit produire un document qui décrit son processus de filtrage de sécurité du personnel. Ce processus doit contenir, au minimum :

(a) Une description des postes des employés et des sous--traitants qui ont besoin d'un accès aux données du Canada ou qui ont la capacité d'influencer la confidentialité, l'intégrité ou la disponibilité des services infonuagiques;

(b) Une description des activités et pratiques du processus de filtrage de sécurité, y compris les procédures de notification qui doivent être suivies si le filtrage n'a pas été achevé ou si les résultats provoquent des doutes ou des préoccupations;

(c) Une description de la sensibilisation et de la formation à la sécurité dans le cadre de l'intégration des employés, lorsque les rôles des employés et des sous-traitants changent, et de façon continue, pour s'assurer que les employés et les sous-traitants comprennent, connaissent et assument leurs responsabilités en matière de sécurité de l'information;

(d) Une description du processus qui est appliqué lorsqu'un employé ou un sous-traitant change de rôle ou au moment d'une cessation d'emploi;

(e) L'approche de détection des employés en place potentiellement malveillants et les contrôles mis en œuvre pour atténuer le risque d'accès aux données du GC ou de dommage à la fiabilité des services infonuagiques hébergeant les données du Canada.

29. Sécurité physique (centre de données/installations)

(1) L'entrepreneur doit veiller à ce que des mesures de sécurité physique soient mises en œuvre pour protéger contre toute forme d'altération, de perte, de dommage et de saisie, les installations de TI et les actifs des systèmes d'information sur lesquels les données du Canada sont stockées et traitées. Des mesures de protection physique visant toutes les installations qui abritent des données du Canada doivent être appliquées selon une approche adaptée fondée sur les risques et reposant sur la prévention, la détection, l'intervention et la récupération en matière de sécurité physique, conformément aux contrôles et aux pratiques en matière de sécurité physique figurant à l'appendice C : Procédures obligatoires relatives aux mesures de sécurité matérielle (https://www.tbs-sct.gc.ca/pol/doc-fra.aspx?id=32611) de la Directive sur la gestion de la sécurité du Conseil du Trésor. Les mesures de sécurité exigées en vertu de cette disposition comprennent, à tout le moins :

(a) Des capacités suffisantes de redondance et de reprise dans et entre les installations de l'entrepreneur, qui sont notamment suffisamment disparates sur le plan géographique pour que la perte d'une installation n'empêche pas la récupération des données du Canada conformément aux engagements de niveau de service prescrits;

(b) L'utilisation adéquate des supports de TI;

(c) Le contrôle de la maintenance de tous les systèmes d'information et de leurs composants pour protéger leur intégrité et assurer leur disponibilité continue;

(d) Le contrôle de l'accès aux périphériques de sortie des systèmes d'information pour empêcher l'accès non autorisé aux données du Canada;

(e) La restriction de l'accès physique aux données du Canada et aux points de prestation des services au personnel des services infonuagiques autorisé en

fonction du poste ou du rôle et du principe du besoin d'accès, validé par deux formes d'identification;

(f) L'accompagnement des visiteurs et la surveillance de leurs activités;

(g) L'application de mesures de protection des données du gouvernement du Canada à d'autres lieux de travail (p. ex. les sites de télétravail);

(h) La consignation et la surveillance de tous les accès physiques aux points de prestation des services et de tous les accès par voie électronique aux systèmes qui hébergent les données du Canada, au moyen d'une combinaison de registres d'accès et de vidéosurveillance dans toutes les zones fragiles, ainsi que de mécanismes de détection des intrusions.

(2) À la demande du Canada, l'entrepreneur doit produire un document qui décrit ses mesures de sécurité physique.

(3) Si des changements apportés aux mesures de sécurité physique sont susceptibles de compromettre considérablement à cette dernière, l'entrepreneur doit en informer le Canada.

30. Gestion des risques liés à la chaîne d'approvisionnement

(1) L'entrepreneur doit prendre des mesures de protection pour atténuer les menaces et les vulnérabilités associées à la chaîne d'approvisionnement des services de TI en vue de préserver la confiance en ce qui concerne la sécurité des sources des systèmes d'information et les composants de TI servant à offrir les services infonuagiques. En font notamment partie la conception et la mise en œuvre de contrôles visant à atténuer et à contenir les risques liés à la sécurité des données par une séparation adéquate des tâches, un accès établi selon les fonctions des utilisateurs et un accès qui suit le principe du privilège minimal pour tout le personnel au sein de la chaîne d'approvisionnement.

(2) L'entrepreneur doit disposer d'une approche de la gestion des risques liés à la chaîne d'approvisionnement, y compris un plan de gestion des risques liés à la chaîne d'approvisionnement orienté en fonction de l'une des pratiques exemplaires suivantes :

(i) ISO/IEC 27036 Technologies de l'information — Techniques de sécurité — Sécurité d'information pour la relation avec le fournisseur (parties 1 à 4);

(ii) NIST Special Publication 800-161 – Supply Chain Risk Management Practices for Federal Information Systems and Organizations;

(iii) Contrôle de sécurité ITSG-33 pour SA-12 lorsque les garanties de sécurité définies sont documentées dans un plan de gestion des risques liés à la chaîne d'approvisionnement.

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

(a) Présenter une preuve selon laquelle l'approche et le plan de gestion des risques liés à la chaîne d'approvisionnement ont été évalués et validés par un tiers indépendant certifié selon les exigences de l'AICPA, de CPA Canada ou du régime de certification ISO.

OU

(b) Fournir au Canada une copie du plan de gestion des risques liés à la chaîne d'approvisionnement sur une base annuelle ou sur demande.

(4) Dans le cas où l'entrepreneur est un fournisseur SaaS qui utilise un fournisseur IaaS approuvé par le GC et qui se conforme déjà aux exigences de l'article 31 — Gestion des risques liés à la chaîne d'approvisionnement, dans les 90 jours suivant l'attribution du contrat, le fournisseur SaaS qui fait appel à un fournisseur IaaS doit fournir une liste de produits de technologie de l'information et de la communication (TIC) décrivant l'équipement de TIC déployé dans l'environnement du fournisseur IaaS approuvé par le GC aux fins d'examen de l'intégrité de la chaîne d'approvisionnement. Cet examen de l'intégrité de la chaîne d'approvisionnement sera effectué au plus tôt tous les trois ans.

31. Sous-traitants

(1) L'entrepreneur doit fournir une liste de sous-traitants auxquels il pourrait faire appel pour exécuter n'importe quelle tâche des services infonuagiques en fournissant le service au Canada. La liste doit comprendre les renseignements suivants : i) le nom du sous-traitant; ii) la description des tâches qui seraient exécutées par le sous-traitant; et iii) les emplacements où le sous-traitant exécuterait les tâches.

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

32. Programme de sécurité industrielle — Exigences relatives à la sécurité pour les fournisseurs canadiens

(1) L'entrepreneur doit détenir en permanence, pendant la réalisation du contrat, de l'offre à commandes ou de l'arrangement en matière d'approvisionnement, une attestation de vérification d'organisation désignée (VOD) en vigueur, ainsi qu'une cote de protection des documents approuvée au niveau PROTÉGÉ B, délivrée par la Direction de la sécurité industrielle canadienne (DSIC), de **Services publics et Approvisionnement Canada (SPAC)**.

(2) Les membres du personnel de l'entrepreneur devant accéder à des renseignements, à des biens ou à des lieux de travail de niveau PROTÉGÉ doivent TOUS détenir une cote de sécurité du personnel valide au niveau SECRET ou FIABILITÉ selon la classification de sécurité, délivrée ou approuvée par la DSIC-SPAC.

(3) L'entrepreneur NE DOIT PAS utiliser ses systèmes de technologie de l'information pour traiter, produire ou stocker électroniquement des renseignements PROTÉGÉS tant qu'il n'en a pas reçu l'approbation écrite par le responsable de la sécurité du ministère client. Lorsque cette approbation aura été accordée, ces tâches pourront être exécutées au niveau PROTÉGÉ B, y compris un lien électronique au niveau PROTÉGÉ B.

(4) L'entrepreneur ou l'offrant doit respecter les dispositions suivantes :

(a) Liste de vérification relative à la sécurité et guide de sécurité (le cas échéant);

(b) Manuel de la sécurité industrielle (dernière édition);

(c) Site Web de la DSIC; Exigences de sécurité des contrats du gouvernement du Canada, disponibles à l'adresse : https://www.tpsgc-pwgsc.gc.ca/esc-src/index-fra.html

REMARQUE : Il y a plusieurs niveaux d'enquête de sécurité du personnel liés à ce dossier. Dans le cas présent, un guide de sécurité doit être ajouté à la LVERS afin d'apporter des précisions sur ces niveaux d'enquête de sécurité. Le guide de sécurité est normalement rédigé par le chargé de projet ou le responsable de la sécurité de l'organisation.

33. Programme de sécurité industrielle — Exigences relatives à la sécurité pour les fournisseurs étrangers

L'administration désignée en matière de sécurité canadienne (ADS canadienne) pour les questions de sécurité industrielle au Canada est le Secteur de la sécurité industrielle (SSI), Services publics et Approvisionnement Canada (SPAC), administrée par la Direction de la sécurité industrielle internationale (DSII), SPAC. L'ADS canadienne est chargée d'évaluer la conformité des entrepreneurs et sous-traitants aux exigences en matière de sécurité pour les fournisseurs étrangers. Les exigences suivantes en matière de sécurité s'appliquent aux **entrepreneurs et sous-traitants** destinataires étrangers constitués en société ou autorisés à faire des affaires dans un État autre que le Canada et qui livrent ou exécutent à l'extérieur du Canada les services infonuagiques décrits dans les solutions d'infonuagique, en plus des exigences en matière de confidentialité et de sécurité. Ces exigences en matière de sécurité s'ajoutent aux exigences figurant dans la section intitulée Protection et sécurité des données stockées dans des bases de données.

(1) **L'entrepreneur ou le sous-traitant** atteste que la livraison et a prestation des services infonuagiques prévus par le présent contrat doit provenir d'un pays membre de l'Organisation du Traité de l'Atlantique Nord (OTAN), de l'Union européenne (UE) ou d'un pays avec lequel le Canada a conclu une entente internationale bilatérale sur la sécurité. Dans le cadre du Programme de sécurité des contrats (PSC), des accords internationaux bilatéraux en matière de sécurité ont été conclus avec les pays énumérés sur le site Web https://www.tpsgc-pwgsc.gc.ca/esc-src/international-fra.html de SPAC, tel qu'il est mis à jour de temps à autre.

(2) **L'entrepreneur ou le sous-traitant** destinataire étranger doit en tout temps, au cours de la durée du **contrat** ou du **contrat de sous-traitance**, être inscrit auprès de l'autorité nationale de supervision appropriée des pays dans lesquels il est constitué en société, exerce ses activités et est autorisé à faire des affaires. Il doit fournir à l'autorité contractante et à l'ADS canadienne la preuve de son inscription auprès de l'autorité de surveillance compétente.

(3) **L'entrepreneur ou le sous-traitant** destinataire étranger doit détenir en permanence, pendant l'exécution du contrat, une équivalence d'une attestation de vérification d'organisation désignée en vigueur, délivrée par l'ADS canadienne, comme suit :

(a) **L'entrepreneur ou le sous-traitant** destinataire étranger doit fournir une preuve qu'il est constitué en société ou autorisé à faire affaire sur son territoire de compétence.

(b) **L'entrepreneur ou le sous-traitant** destinataire étranger doit désigner un agent de sécurité des contrats (ASC) autorisé et un agent remplaçant de sécurité des contrats (ARSC), au besoin, qui sera responsable du contrôle les exigences relatives à la sécurité, telles qu'elles sont définies dans le présent contrat. Cette

personne sera désignée par le président-directeur général ou par un cadre supérieur clé désigné de **l'entrepreneur ou du sous-traitant** destinataire étranger proposant. Les cadres supérieurs clés comprennent les propriétaires, les mandataires, les directeurs, les cadres et les partenaires occupant un poste qui leur permettraient de porter atteinte aux politiques ou aux pratiques de l'organisation durant l'exécution du contrat.

(c) **L'entrepreneur ou le sous-traitant** ne doit pas accorder l'accès aux renseignements et aux biens **PROTÉGÉ B du CANADA**, sauf aux employés ayant un besoin de savoir dans le cadre de l'exécution du **contrat** et qui ont fait l'objet d'une vérification de sécurité conformément à la définition et aux pratiques énoncées dans la *Norme sur le filtrage de sécurité* du Conseil du Trésor (https://www.tbs-sct.gc.ca/pol/doc-fra.aspx?id=28115-), ou doit utiliser des mesures équivalentes acceptables convenues par le Canada.

(d) L'information et les biens **PROTÉGÉS PAR LE CANADA** fournis à **l'entrepreneur ou au sous-traitant** destinataire étranger ou produits par **l'entrepreneur ou sous-traitant** destinataire étranger

i. ne doivent pas être divulgués à un autre gouvernement, à une autre personne ou à une autre entreprise ou à un représentant de l'un ou de l'autre qui ne soit pas directement lié à l'exécution du **contrat**, sans l'autorisation écrite préalable du gouvernement. Ce consentement doit être obtenu auprès de l'ADS canadienne en collaboration avec l'autorité contractante;

ii. ne doivent pas servir à un but autre que l'exécution du contrat sans l'approbation écrite préalable du Canada. Cette approbation doit être obtenue auprès de l'autorité contractante (en collaboration avec l'ADS canadienne).

(4) **L'entrepreneur ou le sous-traitant** destinataire étranger NE DOIT PAS emporter de renseignements ou d'actifs **PROTÉGÉS DU CANADA** hors des lieux de travail visés, et **l'entrepreneur ou le sous-traitant** destinataire étranger doit s'assurer que son personnel est au courant de cette restriction et qu'il la respecte.

(5) **L'entrepreneur ou le sous-traitant** destinataire étranger ne doit pas utiliser les renseignements ni les biens de niveau **PROTÉGÉ AU CANADA** dans un but autre que l'exécution du **contrat** sans l'approbation écrite préalable du gouvernement du Canada. Cette autorisation doit être obtenue auprès de l'ADS canadienne.

(6) **L'entrepreneur ou le sous-traitant** destinataire étranger doit détenir en permanence, pendant l'exécution du **contrat**, une autorisation de détenir des renseignements (ADR) approuvée de niveau **PROTÉGÉ B AU CANADA**.

(7) **L'entrepreneur ou le sous--traitant** destinataire étranger doit se conformer aux dispositions de la Liste de vérification des exigences relatives à la sécurité.

(8) Le Canada a le droit de rejeter toute demande présentée de manière distincte et indépendante de l'autorisation contenue dans le présent contrat relativement à l'autorisation de l'entrepreneur qui fournit les services infonuagiques d'accéder, de traiter, de produire, de transmettre ou de stocker électroniquement des données **PROTÉGÉES DU CANADA** dans tout autre pays s'il y a lieu de craindre pour la sécurité, la confidentialité ou l'intégrité des renseignements.