Annexe 1 – Obligations en matière de sécurité au palier 2 (jusqu'au niveau Protégé B)

1. Généralités

1.1 Objet

La présente annexe a pour objet d'énoncer les obligations du contracteur relativement à la bonne gestion des données du Canada, y compris la protection contre la modification, l'accès ou l'exfiltration non autorisés, conformément à l'entente, à la présente annexe et aux mesures de sécurité du contracteur (collectivement, les **« Obligations en matière de sécurité »**).

1.2 Transfert des obligations en matière de sécurité

Dans la mesure du possible, les obligations du contracteur contenues dans les présentes obligations en matière de sécurité doivent être transférées par le contracteur aux sous-traitants.

1.3 *Gestion du changement*

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

Le contracteur doit informer le Canada de tous les changements qui dégradent sensiblement ou qui peuvent toucher de façon négative les services infonuagiques offerts dans le cadre du présent contrat, y compris les changements ou améliorations de nature technologique, administrative ou autre. Le contracteur s'engage à offrir toutes les améliorations qu'il propose à l'ensemble de ses clients dans le cadre de son offre de services standard, sans frais supplémentaires pour le Canada.

2. Attestation

Les parties reconnaissent que :

(a) les données du Canada sont assujetties à ces obligations en matière de sécurité.

(b) nonobstant toute autre disposition de la présente annexe, les parties ont la responsabilité partagée de l'élaboration et du maintien des politiques, des procédures et des contrôles de sécurité relatifs aux données du Canada.

(c) le contracteur ne doit pas avoir ou tenter d'obtenir la garde de données du Canada, ni permettre à un membre du personnel des services infonuagiques d'accéder aux

données du Canada avant la mise en œuvre des exigences relatives à la sécurité, comme l'exige la présente annexe, au moment de l'attribution du contrat ou avant.

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

3. Protection des données du Canada

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

4. Rôles et responsabilités liés à la sécurité

(1) Le contracteur doit clairement délimiter les rôles et les responsabilités liés aux contrôles et caractéristiques de sécurité des services infonuagiques entre le contracteur et le Canada. Cela comprend, au minimum, les rôles et les responsabilités de chacun concernant : (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) Le contracteur doit fournir au Canada un document à jour qui délimite les rôles et les responsabilités : (i) lors de l'attribution du contrat; (ii) sur une base annuelle; (iii) lorsque ces rôles et responsabilités sont modifiés de façon importante à la suite d'une modification des services d'infonuagique; ou (iv) à la demande du Canada.

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

(1) Le contracteur doit s'assurer que les données du Canada, l'infrastructure du contracteur (y compris tout service IaaS, PaaS ou SaaS fourni au Canada) et les emplacements des services sont protégés par des mesures de sécurité appropriées qui sont conformes aux exigences énoncées dans les pratiques et les politiques du contracteur en matière de sécurité.

(2) Le contracteur doit démontrer que les mesures sont conformes aux exigences énoncées dans les certifications et les rapports de vérification suivants, en fournissant des rapports d'évaluation ou des certifications de tiers indépendants

qui portent sur chaque couche de service (par exemple IaaS, PaaS, SaaS) au sein de l'offre de services infonuagiques, y compris :

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

(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 l'ISO/IEC 27002 pour les services infonuagiques réalisés par un organisme de certification accrédité;

(c) Contrôles au niveau du système et au niveau organisationnel de l'AICPA (Service Organization Control) (SOC) 2 Type II 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 professionnel agréé indépendant.

(3) Chaque rapport de certification ou de vérification fourni doit : (i) indiquer la raison sociale légale du contracteur ou du sous-traitant concerné; (ii) indiquer la date de certification du contracteur ou du sous-traitant et l'état de cette certification; (iii) indiquer les services inclus dans le champ d'application du rapport de certification. Si la méthode créée est utilisée pour exclure des organismes de sous-services tels que l'hébergement de centres de données, le rapport d'évaluation de l'organisme de sous-services doit être inclus.

(4) Chaque vérification donnera lieu à la production d'un rapport qui devra être mis à la disposition du Canada. Les certifications doivent être accompagnées de preuves à l'appui telles que le rapport d'évaluation ISO élaboré pour valider la conformité à la certification ISO et doivent clairement divulguer toute constatation importante faite par le vérificateur. Le contracteur doit remédier rapidement aux problèmes soulevés dans tout rapport de vérification à la satisfaction du vérificateur.

(5) Chaque rapport de vérification SOC 2 de type II doit avoir été réalisé dans les 12 mois précédant le début du contrat. Une lettre de transition peut être fournie pour démontrer que l'entrepreneur
est en cours de renouvellement lorsqu'il y a un décalage entre la date du rapport de l'organisme de services et la fin de l'exercice de l'organisme utilisateur (c'est-à-dire la fin de l'année civile ou de l'exercice financier).

(6) Le contracteur doit maintenir la validité de sa certification ISO 27001, ISO 27017 et SOC 2 Type II pendant toute la durée du contrat. Le contracteur doit fournir, au moins une fois par an, et sans délai à la demande du Canada, tous les rapports ou

dossiers qui peuvent être raisonnablement requis pour démontrer que les certifications du contracteur sont à jour et valides.

6. Vérification de la conformité

(1) Le contracteur doit effectuer les vérifications de la confidentialité et de la sécurité des ordinateurs, de l'environnement informatique et des centres de données physiques qu'il utilise pour traiter et protéger les données du Canada, comme suit :

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

(b) chaque vérification sera réalisée 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 des vérificateurs indépendants, tiers, qui (i) sont qualifiés dans le cadre du régime de certification AICPA, CPA Canada ou ISO, et (ii) sont conformes à la norme ISO/IEC 17020 sur les systèmes de gestion de la qualité, au choix et aux frais du contracteur.

(2) Chaque vérification donnera lieu à la production d'un rapport de vérification qui devra être mis à la disposition du Canada. Le rapport de vérification doit clairement divulguer toute constatation importante faite par le tiers vérificateur. Le contracteur doit, à ses propres frais, remédier rapidement aux problèmes et corriger les lacunes soulevées dans tout rapport de vérification à la satisfaction du vérificateur.

(3) À la demande du Canada, le contracteur ou un sous-traitant peut fournir des preuves supplémentaires du contracteur, y compris des plans de sécurité du système, des conceptions ou des documents d'architecture qui fournissent une description complète du système, afin de compléter les rapports de certification et de vérification décrits à la section 5 (Assurance d'une tierce partie) et de démontrer que le contracteur se conforme aux certifications requises de l'industrie.

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

(1) Le contracteur doit démontrer qu'il respecte les exigences relatives à la sécurité sélectionnées dans le Profil de contrôle de sécurité pour les services de la TI du gouvernement du Canada fondés sur l'infonuagique dans le cas des services non classifiés, intégrité faible et disponibilité faible (NID)

(https://www.canada.ca/en/government/system/digital-government/modern-emergingtechnologies/cloud-computing/government-canada-security-control-profile-cloud-based-itservices.html) pour 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 déterminées ci-dessous, et être validée par des évaluations indépendantes par des tiers.

(2) La conformité sera évaluée et validée par le biais du processus d'évaluation de la sécurité des technologies de l'information (ITSM.50.100) du Centre canadien pour la sécurité cybernétique (CCC) (https://cyber.gc.ca/en/guidance/cloud-servicefournisseur-information-technologie-sécurité-évaluation-processus-itsm50100).

Le contracteur doit démontrer qu'il a participé au processus en adhérant avec succès au programme, en y participant et en le terminant. Il faut à cette fin fournir les documents suivants :

(i) une copie de la lettre de confirmation qui atteste qu'ils ont 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.

Le contracteur doit contacter le service à la clientèle du CCC pour toute information supplémentaire relative au programme d'évaluation des TI du FSI.

Le contracteur des services infonuagiques proposés a l'obligation permanente d'informer le CCC lorsqu'il y a des changements importants dans sa prestation de services de sécurité des TI à l'appui de l'offre du contracteur.

8. Protection des données

(1) Le contracteur doit fournir la capacité de permettre au Canada de faire ce qui suit :

(a) Mettre en œuvre le chiffrement des données inactives pour les services infonuagiques hébergeant les données du Canada, où le chiffrement des données inactives reste en vigueur, ininterrompu et actif en tout temps, même en cas de panne d'équipement ou de problème technique, conformément à la section 13 – Protection cryptographique.

(b) Transmettre les données du Canada de façon sécuritaire, y compris la capacité pour le gouvernement du Canada de mettre en œuvre le chiffrement des données en transit 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.

(2) Le contracteur doit :

(a) Mettre en place des contrôles de sécurité qui limitent l'accès administratif aux données et aux systèmes du Canada par l'entrepreneur et qui donnent la capacité d'exiger l'approbation du Canada avant que le contracteur puisse accéder aux données du Canada pour effectuer des activités de soutien, de maintenance ou d'exploitation.

(b) Prendre des mesures raisonnables pour s'assurer que le personnel du contracteur n'a pas de droits d'accès permanents ou continus aux données du Canada, et que l'accès est limité au personnel du contracteur qui a besoin de connaître, y compris les ressources qui fournissent un soutien technique ou à la clientèle, sur approbation du Canada.

(3) Le contracteur ne doit faire aucune copie des bases de données ou de toute partie de ces bases de données contenant les données du Canada en dehors des capacités de résilience du service régulier et dans les zones ou espaces régionaux approuvés au Canada.

(4) Le contracteur ne doit pas déplacer ou transmettre les copies approuvées en dehors des régions de service convenues, sauf si l'approbation est obtenue du Canada.

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

9. Isolement des données

(1) Le contracteur doit mettre en place des contrôles afin d'assurer un isolement approprié des ressources de sorte que les données du Canada ne se retrouvent pas mêlées aux données d'autres locataires, pendant leur utilisation, leur stockage ou leur transit, et dans tous les aspects de la fonctionnalité de l'infrastructure du contracteur et des services infonuagiques, ainsi que de l'administration des systèmes. Il s'agit notamment de mettre en œuvre des contrôles d'accès et d'appliquer une séparation logique ou matérielle appropriée pour soutenir :

(a) la séparation entre l'administration interne du contracteur 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 n'aient de répercussions sur le service ou les données d'un autre;

(c) la capacité pour le gouvernement du Canada de soutenir l'isolement dans un environnement de locataires géré par le gouvernement du Canada.

(2) À la demande du Canada, le contracteur doit lui fournir un document qui décrit l'approche à adopter pour assurer un isolement approprié des ressources, de sorte que les données du Canada ne se retrouvent pas mêlées aux données d'autres locataires, pendant leur utilisation, leur stockage ou leur transit.

10. Emplacement des données

(1) Le contracteur doit avoir la capacité de stocker et de protéger les données du Canada inactives, y compris les données sauvegardées ou conservées aux fins de redondance. Cela inclut la possibilité d'isoler les données au Canada dans des centres de données approuvés. Un centre de données approuvé est défini comme suit :

a. Un centre de données qui répond à toutes les exigences et certifications de sécurité indiquées à la section 30 pour la sécurité physique (centre de données/installations)

b. qui garantit l'impossibilité de trouver les données d'un client précis sur un support physique;

c. qui utilise le chiffrement pour s'assurer qu'aucune donnée n'est gravée sur disque sous une forme non chiffrée, conformément à la section 13 - Protection cryptographique.

(2) Le contracteur doit attester que la prestation des services infonuagiques dans le cadre du présent contrat provient de pays membres de l'Organisation du traité de l'Atlantique Nord (OTAN) (https://www.nato.int/cps/fr/natohq/nato_countries.htm) ou de l'Union européenne (UE) (https://europa.eu/european-union/about-eu/countries_fr), ou de pays avec lesquels le Canada dispose d'un instrument international bilatéral de sécurité industrielle. Le Programme de sécurité des contrats (PSC) dispose d'instruments bilatéraux internationaux de sécurité industrielle avec les pays énumérés sur le site Web de SPAC suivant : http://www.tpsgc-pwgsc.gc.ca/esc-src/international-fra.html et mis à jour de temps en temps.

(3) Le contracteur doit avoir la capacité pour le Canada d'isoler les données du Canada hébergées dans les services infonuagiques dans des centres de données qui sont géographiquement situés au Canada.

(4) À la demande du Canada, le contracteur doit :

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

b. déterminer 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 le contracteur gère le service.

(5) Le contracteur des services infonuagiques proposés a l'obligation permanente de notifier le

Canada lorsqu'il y a des mises à jour de la liste des lieux physiques où peuvent se trouver les données du Canada.

11. Transfert et récupération des données

Le contracteur doit fournir la capacité, y compris les outils et les services qui permettent au Canada de faire ce qui suit :

(a) Extraire toutes les données du Canada en ligne, de proximité et hors ligne, y compris, mais sans s'y limiter, les bases de données, le stockage d'objets et de fichiers, les configurations de système, les journaux d'activités dans le nuage, le code source hébergé dans un dépôt de codes du Canada et les configurations du réseau de telle sorte que tout utilisateur final du Canada puisse utiliser ces instructions pour migrer d'un environnement à un autre;

(b) Transférer en toute sécurité toutes les données du Canada, y compris les données de contenu et les métadonnées connexes, dans un format lisible et utilisable par machine, notamment le format CSV, et conformément aux Lignes directrices sur les formats de fichier à utiliser pour transférer des ressources documentaires de Bibliothèque et Archives Canada (https://www.bac-lac.gc.ca/fra/services/gestionressources-documentaires/gouvernement/lignes directrices/Pages/lignes directrices-format-fichier--transferers-ressources-documentaires.aspx).

12. Élimination des données et retour des dossiers au Canada

(1) Le contracteur doit éliminer ou réutiliser de façon sécuritaire les ressources (p. ex., l'équipement, le stockage des données, les fichiers et la mémoire) qui contiennent les données du Canada et s'assurer que les données stockées antérieurement ne peuvent être traitées par d'autres clients après leur diffusion. Cela comprend toutes les copies des données du Canada qui sont créées par réplication pour permettre une disponibilité accrue et la reprise après sinistre. L'élimination ou la réutilisation des ressources par le contracteur doit être harmonisée à l'un des documents suivants :

(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 (ITSG-06 du CST). À la demande du Canada, le contracteur doit fournir un document qui décrit le processus d'élimination ou de réutilisation des ressources du contracteur.

(2) Le contracteur doit fournir au Canada une confirmation qui démontre 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 enlevée ou détruite une fois que le Canada aura cessé d'utiliser les services d'informatique en nuage.

13. Protection cryptographique

Le contracteur doit :

(a) configurer toute cryptographie utilisée pour mettre en œuvre des garanties de confidentialité ou d'intégrité, ou utilisée dans le cadre d'un mécanisme d'authentification (par exemple, solutions RVP, TLS, modules logiciels, ICP et jetons d'authentification le cas échéant), conformément aux algorithmes de chiffrement approuvés par le Centre de sécurité des télécommunications (CST), ainsi qu'aux tailles des clés de chiffrement et aux cryptopériodes;

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

(c) S'assurer que la cryptographie validée par la FIPS 140 est utilisée lorsque le 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://www.cse-cst.gc.ca/fr/group-groupe/programme-validation-modules-cryptographiques-pvmc), dans un mode soit approuvé soit autorisé pour fournir un degré élevé de certitude que le module cryptographique validé par la FIPS 140-2 fournit les services de sécurité attendus de la manière prévue;

(d) s'assurer que tous les modules utilisés validés par la FIPS 140-2 ont une certification active, actuelle et valide. Les produits conformes/validés par la FIPS 140 porteront des numéros de certificat.

14. Gestion des clés

Le contracteur doit fournir au Canada un service de gestion des clés qui fournit :

(a) une création/génération et suppression des clés de chiffrement par le gouvernement du Canada;

(b) une définition et application de politiques précises qui contrôlent la manière dont les clés peuvent être utilisées;

(c) une protection de l'accès au matériel de chiffrement, y compris la prévention de l'accès du contracteur au matériel de chiffrement en clair;

(d) une capacité de vérifier tous les événements liés aux services de gestion des clés, y compris l'accès des contracteurs pour l'examen du Canada;

(e) une possibilité d'importer en toute sécurité des clés générées par le gouvernement du Canada à partir d'un module de sécurité du matériel (HSM) géré par le gouvernement du Canada sur place, sans exposer le texte en clair des clés pendant le processus d'importation;

(f) la possibilité d'empêcher le fournisseur de services infonuagiques de récupérer des copies en texte clair des clés générées par le gouvernement du Canada;

(g) la possibilité de déléguer les privilèges d'utilisation des clés aux services infonuagiques utilisés pour les services gérés par le gouvernement du Canada.

15. Protection des points terminaux

Le contracteur doit mettre en œuvre, gérer et surveiller les points terminaux à sécurité renforcée avec des protections actives fondées sur l'hôte pour prévenir les logiciels malveillants, les attaques et les abus, conformément aux directives de configuration reconnues par l'industrie, telles que celles qui se trouvent dans le NIST 800-123 (Guide to General Server Security), les normes du Center for Internet Security (CIS) ou une norme équivalente approuvée par écrit par le Canada.

16. Développement sécurisé

Le contracteur 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 du cycle de vie des systèmes d'information et dans le développement de logiciels, de sites Web et de services, et qui est conforme aux normes et aux pratiques exemplaires de l'industrie, telles que (i) NIST, (ii) ISO 27034, (iii) ITSG-33, (iv) SAFECode, ou (v) les normes de l'Open Web Application Security Project (OWASP) telles que

l'Application Security Verification Standard (ASVS) ou une norme équivalente approuvée par écrit par le Canada. À la demande du Canada, le contracteur doit fournir un document qui décrit l'approche et le processus documentés du cycle de vie du développement des logiciels et des systèmes du contracteur.

17. Gestion de l'identité et des droits d'accès

(1) Le contracteur 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 la norme ITSP.30.031 V2 du CST (ou des versions ultérieures) (https://cyber.gc.ca/fr/publications) à l'aide de justificatifs 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) Le contracteur doit avoir la capacité d'établir des défaillances à l'échelle de l'organisation pour gérer les politiques à l'échelle des locataires.

18. Fédération

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

(a) la prise en charge de normes ouvertes pour les protocoles d'authentification tels que le langage SAML (Security Assertion Markup Language) 2.0 et OpenID Connect 1.0, où les justificatifs d'identité de l'utilisateur final et l'authentification aux services infonuagiques relèvent exclusivement du Canada;

(b) la possibilité d'associer des identifiants uniques du Canada (par exemple, un ID unique du Canada, une adresse électronique au Canada, etc.) aux comptes d'utilisateurs correspondants du service d'informatique en nuage.

19. Gestion de l'accès privilégié

(1) Le contracteur doit :

(a) gérer et surveiller l'accès privilégié aux services infonuagiques afin de s'assurer que toutes les interfaces de service dans un environnement multilocataires sont protégées contre tout accès non autorisé, y compris

celles qui sont utilisées pour héberger les services du gouvernement du Canada;

(b) restreindre et minimiser l'accès aux services infonuagiques et aux données du Canada aux seuls appareils autorisés et aux utilisateurs finaux ayant un besoin explicite d'y avoir accès;

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

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

(e) mettre en œuvre des politiques sur les mots de passe pour protéger les justificatifs d'identité contre la compromission par des attaques en ligne ou hors ligne et pour détecter ces attaques en consignant et en surveillant des événements tels que (i) l'utilisation réussie des justificatifs d'identité, (ii) l'utilisation inhabituelle des justificatifs d'identité, et (iii) l'accès à la base de données des mots de passe et l'exfiltration de celle-ci, conformément à l'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);

(f) mettre en œuvre des mécanismes d'authentification multifactorielle pour authentifier les utilisateurs finaux ayant un accès privilégié, conformément à l'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);

(g) mettre en œuvre des mécanismes de contrôle d'accès fondés sur les rôles afin d'attribuer des privilèges qui forment la base de l'accès aux données du Canada;

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

(i) adhérer aux principes du moindre privilège et du besoin de connaître lors de l'octroi de l'accès aux services infonuagiques et aux données du Canada;

(j) utiliser des terminaux à sécurité renforcée (par exemple, ordinateurs, dispositifs d'utilisateurs finaux, serveurs intermédiaires, etc.) qui sont configurés de façon à offrir une fonctionnalité minimale (par exemple, un terminal spécialisé qui ne peut pas être utilisé pour naviguer sur internet ou consulter ses courriels) afin de fournir le soutien et l'administration des services infonuagiques et de l'infrastructure du contracteur;

(k) mettre en œuvre un processus automatisé pour vérifier périodiquement, au minimum, la création, la modification, l'activation, la désactivation et la suppression de comptes;

(l) en cas de cessation d'emploi, résilier ou révoquer les authentificateurs et les autorisations d'accès associés à tout personnel des services.

(2) À la demande du Canada, le contracteur doit fournir un document qui décrit son approche et son processus de gestion et de contrôle de l'accès privilégié aux services d'informatique en nuage.

20. Gestion à distance

(1) Le contracteur doit gérer et surveiller l'administration à distance des services infonuagiques du contracteur qui sont utilisés pour héberger les services du gouvernement du Canada et prendre des mesures raisonnables pour :

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

(b) utiliser des mécanismes cryptographiques pour protéger la confidentialité des sessions d'accès à distance, conformément à la section 13 (Protection cryptographique);

(c) acheminer tous les accès à distance par des points de contrôle d'accès contrôlés, 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 de commandes privilégiées et l'accès à distance aux informations touchant la sécurité.

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

21. Sécurité des réseaux et des communications

Le contracteur doit :

(a) donner au Canada la capacité d'établir des connexions sécurisées aux services en nuage, notamment en assurant la protection des données en transit entre le Canada et le service infonuagique à l'aide de TLS 1.2 ou de versions ultérieures;

(b) utiliser des protocoles, des algorithmes cryptographiques et des certificats à jour et pris en charge, comme il est indiqué dans l'ITSP.40.062 (https://cyber.gc.ca/fr/orientation/conseils-sur-la-configuration-securisee-des-protocoles-reseau-itsp40062) et l'ITSP.40.111 du CST (https://cyber.gc.ca/fr/orientation/algorithmes-cryptographiques-pour-linformation-non-classifie-protege-et-protege-b);

(c) utiliser des certificats adéquatement configurés dans les connexions TLS, conformément aux directives du CST.

(d) donner au Canada la capacité de mettre en œuvre des contrôles d'accès au réseau et des règles de sécurité qui autorisent ou interdisent le trafic réseau vers les ressources du Canada.

22. Connexions spécialisées

Pour l'IaaS, le contracteur doit fournir au gouvernement du Canada la capacité d'établir une connectivité privée redondante aux services infonuagiques. Cela comprend notamment :

(a) établir la connectivité soit directement dans le réseau étendu du gouvernement du Canada, soit par l'intermédiaire du fournisseur de services d'échange de données dans les nuages du gouvernement du Canada situé au 151, rue Front, à Toronto, et/ou au 625 René-Lévesque, à Montréal, ou dans un endroit approuvé par le gouvernement du Canada à l'intérieur des frontières géographiques du Canada;

(b) permettre une sauvegarde complète et des services de reprise après sinistre grâce à des connexions redondantes au sein des centres de données du contracteur et entre ceux-ci;

(c) avoir des liens de connectivité physique qui sont optiques et qui fournissent un minimum de 10 Gb/s avec la possibilité d'ajouter des liens supplémentaires qui fournissent jusqu'à 40 Gb/s au total, avec une connectivité facultative de 100 Gb/s;

(d) prendre en charge la virtualisation et à la multilocation pour toutes les composantes du réseau;

(e) prendre en charge des protocoles dynamiques de routage (BGP) pour toutes les connexions;

(f) prendre en charge les protocoles approuvés par le gouvernement du Canada comme il est indiqué dans :

i. ITSP.40.062 Conseils sur la configuration sécurisée des protocoles réseau, Section 3.1 pour les suites de chiffrement AES
ii. ITSP.40.111 Algorithmes cryptographiques pour l'information NON CLASSIFIÉ, PROTÉGÉ A et PROTÉGÉ B

(g) fournir une description des emplacements géographiques de tous les centres de données au Canada où la capacité est disponible.

23. Accès et vérification

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

(2) Le contracteur doit donner au Canada la capacité d'exporter des journaux d'événements de sécurité pour les services infonuagiques qu'il utilise, à l'appui des opérations du gouvernement du Canada, y compris la surveillance des services infonuagiques et pour l'investigation électronique et la préservation de la preuve.

(3) Le contracteur doit permettre au Canada d'examiner et d'analyser de façon centralisée les dossiers de vérification provenant de multiples composantes des services infonuagiques utilisés par le client. Cela inclut la possibilité pour le Canada de le faire :

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

(b) enregistrer dans les journaux (ou fichiers journaux) les événements de vérification qui sont synchronisés et horodatés en temps universel coordonné (TUC) et

protégés contre tout accès, modification ou suppression non autorisé pendant que les données sont en transit et inactives;

(c) séparer les incidents de sécurité et les journaux pour les différents comptes du Canada afin de permettre à ce dernier de surveiller et de gérer les événements qui se produisent à l'intérieur de ses frontières et qui ont une incidence sur l'instance d'un service en nuage IaaS, PaaS ou SaaS qui lui est fourni par l'entrepreneur ou un sous-traitant;

(d) transmettre les événements et les journaux des locataires canadiens à un système de journaux de vérification centralisé géré par le gouvernement du Canada en utilisant des interfaces de rapport, des protocoles et des formats de données normalisés (par exemple, format d'événement commun (CEF), syslog ou d'autres formats courants de journaux) et des interfaces de protocole d'application qui permettent de récupérer à distance les données des journaux (par exemple, via une interface de base de données utilisant SQL, etc.)

(4) Pour le SaaS, le contracteur doit fournir des interfaces de protocole d'application qui permettent :

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

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

24. Surveillance continue

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

(a) surveiller activement et en permanence les menaces et les vulnérabilités concernant l'infrastructure du contracteur, les points de service ou les données du Canada;

(b) faire tout en son pouvoir pour empêcher les attaques par des mesures de sécurité telles que les protections contre le refus de service;

(c) faire tout en son pouvoir pour détecter les attaques, les incidents de sécurité et d'autres événements anormaux;

(d) cerner l'utilisation et l'accès non autorisés de tous les services d'informatique en nuage, données et éléments qui ont trait aux services infonuagiques IaaS, PaaS ou SaaS du Canada;

(e) gérer et appliquer les correctifs et les mises à jour de sécurité de manière opportune et systématique afin d'atténuer les vulnérabilités et de remédier à tout problème signalé publiquement dans les services infonuagiques ou les bibliothèques que les services infonuagiques utilisent, et fournir des préavis des correctifs conformément aux engagements en matière de niveau de service conclus;

(f) réagir aux menaces et aux attaques contre les services infonuagiques du contracteur, les contenir et rétablir;

(g) le cas échéant, prendre des contremesures proactives, notamment des mesures à la fois préventives et réactives, pour atténuer les menaces.

(2) Les services infonuagiques du contracteur doivent permettre de copier et de transmettre les données des applications du gouvernement du Canada (pour IaaS, PaaS et SaaS) et le trafic réseau du gouvernement du Canada (pour IaaS et PaaS) des services du gouvernement du Canada hébergés en nuage à un endroit prédéterminé (dans le nuage ou dans les locaux du gouvernement du Canada).

(3) Les services infonuagiques du contracteur doivent permettre au Canada de déployer et d'exploiter des logiciels de sécurité pour effectuer une surveillance avancée et atténuer les cybermenaces pour les services infonuagiques du Canada, au niveau de la couche hôte et réseau gérée par le Canada, pour les composantes gérées par le Canada uniquement.

25. Gestion des incidents de sécurité

(1) Le processus d'intervention du contracteur en cas d'incident de sécurité pour les services infonuagiques doit englober le cycle de vie de la gestion des incidents de sécurité de la TI et les pratiques de soutien pour les activités de préparation, de détection, d'analyse, de confinement et de récupération. Cela comprend notamment :

(a) Un processus d'intervention en cas d'incident de sécurité publié et documenté pour examen par le Canada, qui est harmonisé avec l'une des normes suivantes : (i) ISO/IEC 27035:2011 Technologies de l'information -- Techniques de sécurité -- Gestion des incidents de sécurité informatique; ou (ii) NIST SP800-612, Computer Security Incident Handling Guide; ou (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); ou (iv) autres pratiques

exemplaires des normes de l'industrie, si le Canada détermine, à sa discrétion, qu'elles répondent aux exigences relatives à la sécurité du Canada.

(b) Des processus et des procédures documentés sur la façon dont le contracteur relèvera les incidents de sécurité, y donnera suite, y remédiera, dressera un rapport à leur sujet et les signalera au Canada, notamment (i) la portée des incidents de sécurité en matière d'information que l'entrepreneur signalera au Canada; (ii) le degré de divulgation de la détection des incidents de sécurité en matière d'information et les interventions connexes; (iii) le délai cible dans lequel la notification des incidents de sécurité en matière d'information aura lieu; (iv) la procédure de notification des incidents de sécurité en matière d'information; (v) les coordonnées des personnes-ressources pour le traitement des questions relatives aux incidents de sécurité en matière d'information; et (vi) les recours qui s'appliquent si certains incidents de sécurité en matière d'information se produisent.

(c) La capacité pour l'entrepreneur de soutenir les efforts d'enquête du Canada pour toute compromission des utilisateurs ou des données du service qui est relevée.

(d) N'autorise que les représentants désignés du client (par exemple, le Centre des opérations de sécurité de SPC) autorisés par l'autorité technique :

(i) à demander et recevoir un accès discret et des informations associées aux données du client (données d'utilisateur, journaux d'événements système/sécurité, récupération de paquets réseau ou hôte, journaux des composantes de sécurité telles que SDI/IPS/pare-feu, etc.), en texte clair, aux fins de mener des enquêtes;
(ii) la capacité pour le client de suivre le statut d'un événement de sécurité en matière d'information signalée.

(e) des procédures pour répondre aux demandes de preuve numérique potentielles ou d'autres renseignements provenant de l'environnement des services infonuagiques et comprend des procédures médico-légales et des mesures de protection pour la tenue d'une chaîne de possession;

(2) À la demande du Canada, le contracteur doit fournir un document qui décrit le processus d'intervention du contracteur en cas d'incident de sécurité.

(3) Le contracteur doit :

(a) travailler avec les centres des opérations de sécurité du Canada (par exemple, CCC, COS ministériel) sur le confinement, l'éradication et la récupération des incidents de sécurité 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, la durée, les conséquences de l'atteinte, le nom de la personne qui a signalé l'atteinte et celui de la personne à qui l'atteinte a été signalée, et la procédure pour récupérer les données ou le service;

(c) suivre la divulgation des données du Canada, ou permettre au Canada de la suivre, y compris quelles données ont été divulguées, à qui et à quel moment.

(4) Le Canada peut exiger du contracteur des preuves médico-légales pour l'aider dans une enquête du gouvernement du Canada. Le contracteur s'engage à fournir une assistance au gouvernement du Canada dans toute la mesure du possible.

26. Intervention en cas d'incident de sécurité

(1) Le contracteur doit alerter et aviser rapidement le Canada (par téléphone et par courriel) de toute compromission, de toute violation ou de toute preuve comme (i) un incident de sécurité, (ii) une défectuosité liée à la sécurité d'un bien, (iii) un accès irrégulier ou non autorisé à un bien, (iv) la copie à grande échelle d'un bien d'information, ou (v) une autre activité irrégulière relevée par l'entrepreneur qui amène ce dernier à croire raisonnablement qu'un risque de compromission, ou une atteinte à la sécurité ou à la vie privée, est ou peut être imminent, ou si les mesures de protection existantes ont cessé de fonctionner, au cours de la période suivante (7 jours x 24 heures x 365 jours), et sera effectué sans tarder, en tout état de cause, dans les 72 heures, et dans le respect des engagements en matière de niveau de service du contracteur.

(2) Si le contracteur prend connaissance d'une atteinte à la sécurité entraînant la destruction, la perte, l'altération, la divulgation non autorisée de données du client ou de données personnelles pendant leur traitement par le contracteur (chacun étant un « incident de sécurité ») ou l'accès accidentel ou illégal à ces données, le contracteur doit rapidement et sans tarder (i) aviser le Canada de l'incident de sécurité; (ii) enquêter sur l'incident de sécurité et fournir au Canada des renseignements détaillés sur l'incident de sécurité; et (iii) prendre des mesures raisonnables pour en atténuer la cause et pour réduire au minimum tout dommage résultant de l'incident de sécurité.

27. Fuite d'information

(1) Le contracteur doit disposer d'un processus documenté qui décrit son approche en cas de fuite d'information. Le processus doit être harmonisé avec : (i) le contrôle de sécurité ITSG-33 pour IR-9 Intervention en cas de fuite d'information; ou (ii) une autre norme de l'industrie, approuvée par écrit par le Canada. Sans égard à ce qui précède, le processus d'intervention du contracteur en cas de fuite d'information doit comprendre, au minimum :

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

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

(c) un processus permettant de déterminer les systèmes qui pourraient avoir été contaminés par la suite et toute autre mesure prise pour empêcher une nouvelle contamination.

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

28. Test de sécurité et validation

(1) Le contracteur doit disposer d'un processus permettant au Canada d'effectuer une analyse de vulnérabilité ou un test d'intrusion non perturbateur et non destructif de la partie canadienne des composantes du service infonuagique dans l'environnement du contracteur.

(2) Le contracteur doit fournir la capacité d'habiliter une vérification de la sécurité en mode libre-service ou un outil de notation qui permet de mesurer la posture de sécurité des services infonuagiques configurés par le Canada.

29. Filtrage de sécurité du personnel

(1) Le contracteur doit mettre en œuvre des mesures de sécurité qui permettent d'accorder et de maintenir le niveau requis de filtrage de sécurité du personnel du contracteur chargé de la prestation des services infonuagiques et du personnel des sous-traitants conformément à leurs privilèges d'accès aux biens en matière de systèmes d'information dans lesquels les données du Canada sont stockées et traitées.

(2) Les mesures de filtrage du contracteur doivent être appliquées conformément à la définition et aux pratiques de 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, le contracteur doit fournir un document qui décrit le processus de filtrage de sécurité du personnel du contracteur. Le processus doit comprendre, au minimum :

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

(b) une description des activités et des pratiques de filtrage de sécurité, y compris les procédures de notification à suivre si le filtrage n'a pas été effectué au complet ou si les résultats suscitent des doutes ou des inquiétudes;

(c) une description de la sensibilisation et de la formation en matière sécurité à l'accueil 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 leurs responsabilités en matière de sécurité de l'information, en sont conscients et s'en acquittent;

(d) une description du processus qui s'applique lorsqu'un employé ou un sous-traitant change de rôle ou lorsqu'il est mis fin à son emploi;

(e) l'approche de détection de menaces internes potentielles et les contrôles mis en œuvre pour atténuer le risque d'accès aux données du gouvernement du Canada et/ou d'avoir une incidence sur la fiabilité des services infonuagiques qui hébergent les données du Canada.

30. Sécurité matérielle (ou physique) (centre de données/installations)

(1) Le contracteur doit mettre en œuvre des mesures de sécurité matérielle (physique) qui assurent la protection des installations de TI et des biens des systèmes d'information dans lesquels les données du Canada sont stockées et traitées contre toute forme d'altération, de perte, de dommages et de saisie. Des mesures de protection matérielles visant toutes les installations qui hébergent les données du Canada doivent être appliquées conformément à une approche de la sécurité physique fondée sur les risques reposant sur la prévention, la détection, l'intervention et la récupération, harmonisées avec les contrôles et les pratiques de sécurité physique énoncés dans la Norme opérationnelle sur la sécurité matérielle du Conseil du Trésor (https://www.tbs-sct.gc.ca/pol/doc-fra.aspx?id=12329). Les mesures de sécurité requises dans ce cadre comprennent, au minimum :

(i) Des capacités de redondance et de récupération suffisantes au sein des installations du contracteur et entre celles-ci, qui sont géographiquement hétérogènes de sorte que la perte d'une installation n'empêche pas la récupération de données et des données du Canada dans le cadre des engagements en matière de niveau de service prescrit;

(ii) la bonne gestion des supports de TI;

(iii) la maintenance contrôlée de tous les systèmes d'information et de leurs composantes afin de protéger leur intégrité et d'assurer leur disponibilité permanente;

(iv) l'accès contrôlé aux dispositifs de sortie des systèmes d'information afin d'empêcher tout accès non autorisé aux données du Canada;

(v) limiter l'accès physique aux données du Canada et aux points de service au personnel autorisé des services infonuagiques en fonction du poste ou du rôle et du principe du besoin d'accès, et validé par deux formes d'identification;

(vi) escorter les visiteurs et surveiller l'activité des visiteurs;

(vii) appliquer des mesures de protection des données du gouvernement du Canada à d'autres sites de travail (par exemple, les sites de télétravail);

(viii) consigner et surveiller tous les accès physiques aux points de service et tous les accès logiques aux systèmes hébergeant les données du Canada, à l'aide d'une combinaison de journaux d'accès et de vidéosurveillance dans toutes les zones sensibles et de mécanismes de détection d'intrusion.

(2) À la demande du Canada, l'entrepreneur doit fournir un document qui décrit les mesures de sécurité physiques du contracteur.

(3) Si des mesures de sécurité physique doivent être modifiées d'une manière qui dégrade de façon importante la sécurité physique, l'entrepreneur doit en informer le Canada.

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

(1) Le contracteur doit mettre en œuvre des mesures de protection pour atténuer les menaces et les vulnérabilités liées à la chaîne d'approvisionnement concernant les services de TI afin de maintenir la confiance dans la sécurité des sources d'information et des composantes de TI utilisées pour fournir des services infonuagiques. Cela comprend, mais sans s'y limiter, la conception et la mise en œuvre de contrôles visant à atténuer et à contenir les risques pour la sécurité des données par une séparation adéquate des tâches, un accès fondé sur les rôles et un accès qui suit le principe du privilège minimal pour tout le personnel de la chaîne d'approvisionnement.

(2) Le contracteur doit avoir 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 qui est aligné sur l'une des pratiques exemplaires suivantes :

(i) ISO/IEC 27036 Technologies de l'information -- Techniques de sécurité -- Sécurité de l'information dans les relations avec les fournisseurs (parties 1 à 4);

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

(iii) Contrôle de sécurité ITSG-33 pour SA-12 où les mesures de sécurité définies par l'organisation sont documentées dans un plan de GRCA.

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

(a) fournir la preuve que l'approche et le plan de GRCA ont été évalués et validés par un tiers indépendant certifié selon les exigences de l'AICPA ou de CPA Canada, et/ou du régime de certification ISO

OU

(b) fournir tous les ans au Canada une copie du plan de GRCA, ou à la demande du Canada.

(4) Dans le cas où le contracteur est un fournisseur SaaS utilisant un fournisseur IaaS approuvé par le gouvernement du Canada qui se conforme déjà aux exigences de la section 31 – Gestion des risques liés à la chaîne d'approvisionnement, dans les 90 jours suivant l'attribution du contrat, le fournisseur SaaS utilisant
un fournisseur IaaS approuvé par le Canada doit fournir une liste de produits de la technologie de l'information et des communications (TIC) qui décrit l'équipement TIC qui est déployé dans l'environnement du fournisseur IaaS approuvé par le gouvernement du Canada pour un examen de l'intégrité de la chaîne d'approvisionnement (ICA). Cet examen de l'ICA sera effectué au plus tôt tous les trois ans.

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

(1) Le contracteur doit, en tout temps pendant la durée du contrat, de l'offre à commandes ou de l'arrangement en matière d'approvisionnement, détenir une vérification d'organisme désigné valide avec une protection approuvée des documents de niveau PROTÉGÉ B délivrée par la Direction des services industriels des organisations (DSSIO) de **Services publics et Approvisionnement Canada (SPAC).**

(2) Les membres du personnel du contracteur demandant l'accès à des renseignements, biens ou sites de travail PROTÉGÉ doivent CHACUN détenir un filtrage de sécurité du personnel valide de niveau SECRET, ou
Une COTE DE FIABILITÉ, tel que l'exige le guide de sécurité, accordée ou approuvée par la DSSIO/SPAC.

(3) Le contracteur NE DOIT PAS utiliser ses systèmes de technologie de l'information pour traiter, produire ou entreposer électroniquement des renseignements PROTÉGÉ sans l'approbation écrite de l'autorité de sécurité du ministère client. Une fois l'approbation accordée, ces tâches peuvent être effectuées au niveau PROTÉGÉ B, y compris un lien électronique au niveau PROTÉGÉ B.

(4) Le contracteur ou l'offrant doit respecter les dispositions de ce qui suit :

(a) la liste de vérification des exigences relatives à la sécurité et le guide de sécurité (le cas échéant) joints à titre d'annexe A et d'annexe B.

(b) le Manuel de la sécurité industrielle (dernière édition).

(c) Site Web de la DSSIO : Exigences de sécurité des contrats du gouvernement du Canada, à l'adresse www.tpsgc-pwgsc.gc.ca/esc-src

REMARQUE : Il existe plusieurs niveaux de filtrage de sécurité du personnel associés à ce dossier. Dans le présent cas, un guide de sécurité doit être ajouté à la LVERS pour clarifier ces filtrages. Le guide de sécurité est normalement généré par le chargé de projet et/ou l'autorité de sécurité de l'organisation.

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

L'autorité de sécurité désignée canadienne (ASD canadienne) pour les questions de sécurité industrielle au Canada est le Secteur de la sécurité industrielle (SSI), Services publics et Approvisionnement Canada (SPAC), administré par la Direction de la sécurité industrielle internationale (DSII), SPAC. L'ASD canadienne est l'autorité chargée de confirmer la conformité du contracteur **ou du sous-traitant** aux exigences relatives à la sécurité pour les fournisseurs étrangers. Les exigences relatives à la sécurité suivantes s'appliquent **au contracteur ou au sous-traitant** destinataire étranger constitué en société ou autorisé à faire des affaires dans un État autre que le Canada et à fournir/exécuter à l'extérieur du Canada les services infonuagiques décrits dans la solution infonuagique, en plus des exigences en matière de protection des renseignements personnels et de sécurité. Ces exigences relatives à la sécurité s'ajoutent à celles indiquées dans la section intitulée « Protection et sécurité des données stockées dans des bases de données ».

(1) **Le contracteur ou le sous-traitant** atteste que la prestation et le provisionnement de services infonuagiques selon les termes de ce contrat doivent provenir d'un pays de l'Organisation du Traité de l'Atlantique Nord (OTAN), de l'Union européenne (UE) ou d'un pays avec lequel le Canada dispose d'une entente bilatérale internationale en matière de sécurité. Le Programme de sécurité des contrats (PSC) dispose d'ententes bilatérales internationales en matière de sécurité avec les pays énumérés sur le site Web de SPAC suivant : http://www.tpsgc-pwgsc.gc.ca/esc-src/international-fra.htmlet mis à jour de temps en temps.

(2) **Le contracteur ou le sous-traitant** destinataire étranger doit, en tout temps pendant l'exécution du **contrat ou contrat de sous-traitance**, être inscrit auprès de l'autorité de surveillance gouvernementale compétente du ou des pays dans lesquels il est constitué en société ou exerce ses activités et autorisé à faire des affaires. **Le contracteur ou sous-traitant** destinataire étranger doit fournir à l'autorité contractante et à l'ASD canadienne une preuve de son inscription auprès de l'autorité de surveillance compétente.

(3) **Le contracteur ou le sous-traitant** destinataire étranger doit, en tout temps pendant l'exécution du **contrat**, détenir une équivalence de vérification d'organisme désignée (VOD) valide, délivrée par l'ASD canadienne comme suit :

(a) **Le contracteur ou le sous-traitant** destinataire étranger doit fournir la preuve qu'il est constitué en société ou autorisé à faire des affaires dans sa compétence.

(b) **Le contracteur ou le sous-traitant** destinataire étranger doit désigner un agent de sécurité des contrats (ASC) autorisé et un agent de sécurité des contrats suppléant (ASCS) (le cas échéant) chargé de la supervision des exigences relatives à la sécurité, telles qu'elles sont définies dans le présent contrat. Cette personne sera nommée par le président-directeur général ou par un cadre supérieur clé désigné **du contracteur ou du sous-traitant** destinataire étranger qui présente une soumission, défini comme étant un propriétaire, un dirigeant, un administrateur, un cadre dirigeant ou un partenaire qui occupe un poste qui lui permettrait de nuire aux politiques ou aux pratiques de l'organisation dans l'exécution du contrat.

(c) **Le contracteur ou le sous-traitant** ne doit pas donner accès aux renseignements ou biens **CANADA PROTÉGÉ B**, sauf au personnel qui a besoin de connaître pour l'exécution du **contrat** et qui a fait l'objet d'un filtrage de sécurité conformément à la définition et aux pratiques de 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 des mesures équivalentes acceptables convenues par le Canada.

(d) Les renseignements ou biens **CANADA PROTÉGÉ** fournis **au contracteur ou au sous-traitant** destinataire étranger ou produits par **le contracteur ou le sous-traitant** destinataire étranger :

i. ne doivent pas être divulgués à un autre gouvernement, une autre personne ou une autre entreprise, ou un de ses représentants qui n'est pas directement lié à l'exécution du **contrat**, sans le consentement écrit préalable du Canada. Ce consentement doit être demandé à l'ASD canadienne en collaboration avec l'autorité contractante;

ii. ne doivent pas être utilisés à d'autres fins que l'exécution du **contrat** sans l'accord écrit préalable du Canada. Cette approbation doit être obtenue en contactant l'autorité contractante (en collaboration avec l'ASD canadienne).

(4) **Le contracteur ou le sous-traitant** destinataire étranger NE DOIT retirer aucun renseignement ou bien **CANADA PROTÉGÉ** du site de travail désigné, et **le contracteur ou le sous-traitant** destinataire étranger doit s'assurer que son personnel est informé de cette restriction et qu'il la respecte.

(5) **Le contracteur ou le sous-traitant** destinataire étranger ne doit pas utiliser les renseignements ou biens **CANADA PROTÉGÉ** à d'autres fins que l'exécution du **contrat** sans l'approbation écrite préalable du gouvernement du Canada. Cette approbation doit être obtenue auprès de l'ASD canadienne.

(6) **Le contracteur ou le sous-traitant** destinataire étranger doit, en tout temps pendant l'exécution du **contrat** détenir une équivalence à une autorisation de détenir des renseignements (ADR) approuvés au niveau de **CANADA PROTÉGÉ B**.

(7) **Le contracteur ou le sous-traitant** destinataire étranger doit se conformer aux dispositions de la Liste de vérification des exigences relatives à la sécurité jointe aux annexes B et C.

(8) Le Canada a le droit de rejeter toute demande présentée séparément et indépendamment de l'autorisation prévue dans le présent contrat en rapport avec le contracteur fournissant les services infonuagiques d'accéder à des données **CANADA PROTÉGÉ** relatives aux services infonuagiques dans tout autre pays s'il y a lieu de craindre pour la sécurité, la confidentialité ou l'intégrité des renseignements, ou de traiter, de produire, de transmettre ou de stocker par voie électronique ces données.