Appendice B – Annexe 1 – Obligations en matière de sécurité dans le cas des services commerciaux d'informatique en nuage (jusqu'au niveau Protégé B inclusivement)

Remarque à l'intention de l'autorité contractante : À moins d'indication contraire, toutes les clauses s'appliquent au travail Non classifié, Protégé A et Protégé B, ainsi qu'aux modèles de prestation de services IaaS/PaaS/SaaS.

1. Généralités

1.1 *Objectif*

La présente annexe fait état des obligations de l'entrepreneur en matière de saine 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 de l'entrepreneur (collectivement, les « **obligations en matière de sécurité** »).

1.2 *Répartition des obligations en matière de sécurité*

Les obligations de l'entrepreneur contenues dans le présent document s'appliquent également à tous les sous-traitants dans la mesure où cela est applicable.

1.3 *Gestion du changement*

L'entrepreneur doit, tout au long du contrat, prendre toutes les mesures nécessaires pour mettre à jour et maintenir les exigences en matière de sécurité en fonction des besoins, afin de se conformer aux pratiques exemplaires en matière de sécurité et aux normes de l'industrie, telles qu'elles sont énoncées dans la présente annexe.

L'entrepreneur doit informer le Canada de tout changement ayant pour effet de dégrader de façon importante les services d'informatique en nuage offerts dans le cadre du présent contrat ou susceptibles d'avoir une incidence négative sur ces services, y compris des changements ou des améliorations d'ordre technologique, administratif ou autre. L'entrepreneur 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. Remerciements

Les parties reconnaissent que :

a) Les données du Canada sont soumises à ces obligations en matière de sécurité.

b) Nonobstant toute autre disposition de la présente annexe, les parties ont la

responsabilité partagée d'élaborer et de maintenir des politiques, des procédures et des contrôles de sécurité en ce qui concerne les données du Canada.

c) L'entrepreneur ne doit pas avoir ou tenter d'obtenir la garde des données du Canada, ni permettre au personnel des services d'informatique en nuage d'accéder aux données du Canada avant la mise en œuvre des exigences en matière de sécurité requises en vertu de la présente annexe, au plus tard à la date d'attribution du contrat.

d) Les obligations en matière de sécurité s'appliquent aux **services commerciaux d'informatique en nuage** (jusqu'aux niveaux Protégé B, Intégrité moyenne, Disponibilité moyenne ou Niveau de préjudice moyen), sauf indication contraire.

3. Sécuriser les données du Canada

(1) L'entrepreneur doit protéger les données du Canada contre l'accès non autorisé, la modification ou l'exfiltration. Pour ce faire, il doit notamment mettre en œuvre et appliquer des mesures de sécurité techniques et organisationnelles appropriées, y compris des politiques, des procédures et des contrôles de sécurité en matière de sécurité de l'information, afin de préserver la confidentialité, l'intégrité et la disponibilité des données du Canada.

4. Rôles et responsabilités en matière de sécurité

(1) L'entrepreneur doit clairement délimiter les rôles et responsabilités de l'entrepreneur et du Canada en ce qui concerne les contrôles et les caractéristiques de sécurité des services d'informatique en nuage. Cela inclut, à tout le moins, les rôles et responsabilités pour ce qui est de : (i) la gestion des comptes; (ii) la protection des limites; (iii) la sauvegarde des actifs et des systèmes d'information; (iv) la gestion des incidents; (v) la surveillance des systèmes; et (vi) la gestion des vulnérabilités.

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

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

(1) L'entrepreneur doit s'assurer que les données du Canada, l'infrastructure de l'entrepreneur (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 respectent les exigences énoncées dans les pratiques et politiques de l'entrepreneur en matière de sécurité.

(2) [S'applique uniquement dans le cas du travail Protégé B et des modèles de prestation de services IaaS/PaaS/SaaS] L'entrepreneur doit démontrer que les mesures sont conformes aux exigences énoncées dans les certifications et les rapports d'audit suivants, en fournissant des rapports d'évaluation ou des certifications de tiers indépendants portant sur chaque niveau de service (par exemple, IaaS, PaaS, SaaS) prévu dans l'offre de services d'informatique en

nuage, notamment :

(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 (ou versions ultérieures); ET

(b) ISO/IEC 27017:2015 Technologies de l'information -- Techniques de sécurité -- Code de bonnes pratiques pour les contrôles de sécurité de l'information fondés sur l'ISO/IEC 27002 pour les services du nuage, obtenu par un organisme de certification accrédité (ou des versions ultérieures); ET

(c) AICPA Service Organization Control (SOC) 2 Rapport d'audit de type II de l'AICPA Service Organization Control (SOC) 2 pour les principes fiduciaires de sécurité, de disponibilité, d'intégrité du traitement et de confidentialité – préparé un expert-comptable indépendant.

(3) [S'applique uniquement dans le cas du travail Protégé A et des modèles de prestation de services PaaS/SaaS] L'entrepreneur doit démontrer que les mesures sont conformes aux exigences énoncées dans les certifications et les rapports d'audit suivants, en fournissant des rapports d'évaluation ou des certifications de tiers indépendants portant sur chaque niveau de service (par exemple, IaaS, PaaS, SaaS) prévu dans de l'offre de services d'informatique en nuage, 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 (ou versions ultérieures); OU

(b) Rapport d'audit de type II de l'AICPA Service Organization Control (SOC) 2 pour les principes fiduciaires de sécurité, de disponibilité, d'intégrité du traitement et de confidentialité – préparé un expert-comptable indépendant; ET

(c) Auto-évaluation, par l'entrepreneur, de la Cloud Security Alliance Cloud Controls Matrix (CCM) v4 (ou versions ultérieures).

(4) [S'applique uniquement dans le cas du travail Non classifié et du modèle de prestation de services SaaS] L'entrepreneur doit démontrer que les mesures sont conformes aux exigences énoncées dans les certifications et les rapports d'audit suivants en fournissant des rapports d'évaluation ou des certifications de tiers indépendants portant sur chaque couche de service (par exemple, IaaS, PaaS, SaaS) au sein de l'offre de services d'informatique en nuage, 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 (ou versions ultérieures); OU

(b) Rapport d'audit de type II de l'AICPA Service Organization Control (SOC) 2 pour les principes fiduciaires de sécurité, de disponibilité, d'intégrité du traitement et de confidentialité – préparé un expert-comptable indépendant; OU

(c) Auto-évaluation, par l'entrepreneur, de la Cloud Security Alliance Cloud Controls Matrix (CCM) v4 (ou versions ultérieures).

(5) Chaque rapport de certification ou d'audit fourni doit indiquer : (i) la raison sociale de l'entrepreneur ou du sous-traitant; (ii) la date de certification de l'entrepreneur ou du sous-traitant et le statut de cette certification; (iii) les services inclus dans la portée du rapport de certification. Si la méthode de découpage 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.

(6) Chaque audit donne lieu à l'établissement d'un rapport d'audit qui doit être mis à la disposition du Canada. Les certifications doivent être accompagnées de pièces justificatives comme le rapport d'évaluation ISO élaboré pour valider la conformité à la certification ISO, et doivent indiquer clairement toutes les constatations importantes faites par l'auditeur. L'entrepreneur doit rapidement remédier aux problèmes soulevés dans tout rapport d'audit, à la satisfaction de l'auditeur, et fournir au Canada avec des preuves à l'appui des mesures correctives prises ou une confirmation de l'auditeur que les problèmes ont été résolus à la satisfaction de l'auditeur.

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

(8) L'entrepreneur est tenu de maintenir sa certification ISO 27001, ISO 27017 et/ou SOC 2 Type II, selon le cas, pendant 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 dossiers pouvant raisonnablement être exigés pour démontrer que les certifications e l'entrepreneur sont à jour et maintenues.

6. Audit de conformité

(1) L'entrepreneur doit s'assurer que des vérifications de la sécurité et de la protection des renseignements personnels des ordinateurs, de l'environnement informatique et des centres de données physiques qu'il utilise pour traiter et protéger les données du Canada sont effectuées comme suit :

a) Lorsqu'une norme ou un cadre prévoit des audits, un audit de cette norme ou de ce cadre de contrôle sera effectué au moins une fois par année.

b) Chaque audit sera réalisé conformément aux normes et règles de l'organisme de réglementation ou d'accréditation pour chaque norme ou cadre de contrôle applicable.

c) Chaque audit sera réalisé par des auditeurs tiers indépendants qui (i) sont

qualifiés selon le régime de certification de l'AICPA, de CPA Canada ou de l'ISO, et (ii) respectent la norme ISO/IEC 17020 relative au système de gestion de la qualité, selon le choix et aux frais de l'entrepreneur.

(2) Chaque audit donne lieu à un rapport d'audit qui doit être mis à la disposition du Canada. Le rapport d'audit doit indiquer clairement toutes les constatations importantes faites par le tiers auditeur. L'entrepreneur doit, à ses propres frais, remédier rapidement aux problèmes et corriger les déficiences soulevées dans tout rapport d'audit, à la satisfaction de l'auditeur.

(3) À la demande du Canada, des preuves supplémentaires de l'entrepreneur, y compris des plans de sécurité des systèmes, des conceptions ou des documents d'architecture offrant une description complète du système, peuvent être fournies par l'entrepreneur ou un sous-traitant secondaire pour compléter les rapports de certification et de vérification décrits à l'article 5 (Assurance par une tierce partie) afin de démontrer que l'entrepreneur est conforme aux certifications requises de l'industrie. Cela inclut les cas où l'entrepreneur est un fournisseur SaaS ou PaaS qui utilise des centres de données physiques fournis par un fournisseur IaaS tiers.

7. Programme d'évaluation de la sécurité informatique des fournisseurs de services d'informatique en nuage (FSN)

(1) [S'applique uniquement dans le cas du travail Protégé B et des modèles de prestation de services IaaS/PaaS/SaaS] L'entrepreneur doit démontrer qu'il respecte les exigences de sécurité de l'annexe B du profil de contrôle de l'informatique en nuage du Centre canadien pour la cybersécurité (CCS) – Guide sur la catégorisation de la sécurité des services fondés sur l'infonuagique (ITSP.50.103) pour la portée des services d'informatique en nuage fournis par le contractant. La conformité doit être démontrée par la mise en correspondance des contrôles de sécurité avec les certifications sectorielles applicables identifiées ci-dessous, et validée par des évaluations de tiers indépendants.

La conformité sera évaluée et validée au moyen du Processus d'évaluation de la sécurité des technologies de l'information s'appliquant aux fournisseurs de services infonuagiques (ITSM.50.100).

L'entrepreneur doit démontrer qu'il a participé au processus en intégrant le programme, en y participant et en le réalisant avec succès. Il s'agit notamment de fournir les documents suivants :

(i) Une copie du plus récent rapport d'évaluation fourni par le Canada
(ii) Une copie du plus récent rapport de synthèse par le Canada.

L'entrepreneur devrait contacter le ministère du gouvernement du Canada responsable de l'approvisionnement pour tout renseignement supplémentaire concernant le programme d'évaluation des technologies de l'information du fournisseur de services.

L'entrepreneur offrant les services d'informatique en nuage proposés est tenu

d'informer le ministère du GC responsable de l'approvisionnement de tout changement important dans le cadre de la prestation de services de sécurité des TI à l'appui de l'offre de l'entrepreneur.

(2) [S'applique uniquement dans le cas du travail Protégé A et des modèles de prestation de services PaaS/SaaS] L'entrepreneur doit démontrer qu'il respecte les exigences de sécurité de l'annexe A du profil de contrôle de l'informatique en nuage du Centre canadien pour la cybersécurité (CCS) – Faible du Guide sur la catégorisation de la sécurité des services fondés sur l'infonuagique (ITSP.50.103). La conformité doit être démontrée par la mise en correspondance des contrôles de sécurité avec les certifications sectorielles applicables indiquées ci-après, et validée au moyen d'évaluations de tiers indépendants.

La conformité sera évaluée et validée au moyen du Processus d'évaluation de la sécurité des technologies de l'information s'appliquant aux fournisseurs de services infonuagiques (ITSM.50.100).

L'entrepreneur doit démontrer qu'il a participé au processus en intégrant le programme, en y participant et en le réalisant avec succès. Il s'agit notamment de fournir les documents suivants :

(i) Une copie du plus récent rapport d'évaluation fourni par le Canada
(ii) Une copie du plus récent rapport de synthèse fourni par le Canada.

L'entrepreneur devrait contacter le ministère du gouvernement du Canada responsable de l'approvisionnement pour tout renseignement supplémentaire concernant le programme d'évaluation des technologies de l'information du fournisseur de services.

L'entrepreneur offrant les services d'informatique en nuage proposés est tenu d'informer le ministère du GC responsable de l'approvisionnement de tout changement important dans le cadre de la prestation de services de sécurité des TI à l'appui de l'offre de l'entrepreneur.

(3) Si l'entrepreneur est un fournisseur de SaaS faisant appel à un fournisseur de IaaS approuvé par le GC et qui se conforme déjà à l'article 5 – Assurance par une tierce partie et à l'article 7 – Programme d'évaluation de la sécurité informatique des fournisseurs de services d'informatique en nuage (FSN), paragraphes (1) et (2), le fournisseur de SaaS doit fournir au Canada une copie d'un courriel émanant du Centre canadien pour la cybersécurité (CCS) confirmant que le soumissionnaire a suivi le programme d'évaluation de la sécurité des TI du CCS. Le courriel doit indiquer que le fournisseur a été évalué par le programme d'évaluation de la sécurité des TI et qu'il a reçu un rapport final concernant l'évaluation. Pour toute question, le CCS peut être contacté par courriel, à l'adresse suivante : contact@cyber.gc.ca.

8. Protection des données

(1) L'entrepreneur doit :

a) Mettre en œuvre le chiffrement des données au repos pour les services d'informatique en nuage hébergeant les données du Canada lorsque le chiffrement des données au repos demeure en vigueur, ininterrompu et actif en tout temps, même en cas de défaillance de l'équipement ou de la technologie, conformément à l'article 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 transit pour toutes les transmissions de données du Canada, conformément à l'article 13 – Protection cryptographique et à l'article 21 – Sécurité des réseaux et des communications.

(2) L'entrepreneur doit :

(a) mettre en œuvre des contrôles de sécurité qui limitent l'accès administratif aux données et systèmes du Canada par l'entrepreneur et la possibilité d'exiger l'autorisation écrite du Canada pour avoir accès aux données du Canada pour effectuer les activités de soutien, de maintenance ou d'exploitation

(b) prendre des mesures raisonnables pour s'assurer que le personnel de l'entrepreneur n'a pas des droits d'accès permanents ou continus aux données du Canada, et que l'accès est limité au personnel de l'entrepreneur ayant besoin d'en connaître, y compris les ressources offrant une assistance technique ou un service à la clientèle, sur approbation du Canada.

(3) L'entrepreneur ne doit pas faire de copies des bases de données ou de toute partie des bases de données contenant les données du Canada en dehors des capacités de résilience des services réguliers et dans le cadre des zones ou espaces réguliers au sein du Canada.

(4) L'entrepreneur ne doit pas déplacer ou transmettre des copies approuvées en dehors des régions approuvées pour les services prévus, à moins d'une autorisation écrite du GC.

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

9. Séparation des données

(1) L'entrepreneur doit mettre en œuvre des contrôles pour assurer une séparation appropriée des ressources afin que les données du Canada ne soient pas mélangées avec les données des autres locataires, pendant leur utilisation, leur stockage ou leur transit, et dans tous les aspects de la fonctionnalité et de l'administration des systèmes des services d'informatique en nuage et de l'infrastructure de l'entrepreneur. Il s'agit notamment de mettre en œuvre des contrôles d'accès et d'appliquer une séparation logique ou physique appropriée pour soutenir les activités :

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

(b) La séparation des ressources des clients en présence de plusieurs locataires, afin d'éviter qu'un locataire malveillant ou compromis n'affecte le service ou les données d'un autre locataire.

(c) (Pour IaaS) Capacité du GC de prendre en charge l'isolation dans l'environnement du locataire géré par le GC.

(2) À la demande du Canada, l'entrepreneur doit fournir au Canada un document qui décrit l'approche adoptée pour assurer une séparation appropriée des ressources de façon à ce que les données du Canada ne soient pas mélangées avec les données d'autres locataires, pendant leur utilisation, leur stockage ou leur transit.

10. Localisation des données

(1) L'entrepreneur doit avoir la capacité de stocker et de protéger les données du Canada, au repos, y compris les données sauvegardées ou conservées à des fins de redondance. Cela inclut la possibilité d'isoler les données au Canada dans des centres de données agréés, c'est-à-dire un centre qui :

a) satisfait à toutes les exigences de sécurité et certifications identifiées dans la section 30 pour la sécurité matérielle (centre de données / installations);

b) garantit qu'il est impossible de trouver les données d'un client spécifique sur un support physique;

c) utilise le chiffrement pour s'assurer e pour s'assurer qu'aucune donnée n'est écrite sur le disque en clair, conformément à l'article 13 – Protection cryptographique

(2) [S'applique uniquement dans le cas du travail Protégé B et des modèles de prestation de services IaaS/PaaS/SaaS] L'entrepreneur doit certifier que la prestation de services d'informatique en nuage dans le cadre du présent contrat est effectuée à partir de pays membres de l'Organisation du traité de l'Atlantique Nord (OTAN), de l'Union européenne ou de pays avec lesquels le Canada a conclu un instrument de sécurité bilatéral. Le Programme de sécurité des contrats de SPAC a conclu des instruments de sécurité bilatéraux avec différents

pays et la liste est mise à jour périodiquement.

(3) [S'applique uniquement dans le cas du travail Protégé B et des modèles de prestation de services IaaS/PaaS/SaaS] L'entrepreneur doit permettre au Canada d'isoler les données du Canada hébergées dans les services d'informatique en nuage dans des centres de données situés géographiquement au Canada.

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

a) [S'applique uniquement dans le cas du travail Protégé A et B et des modèles de prestation de services IaaS/PaaS/SaaS] fournir au GC une liste à jour des emplacements physiques, y compris la ville, susceptibles de contenir des données du Canada pour chaque centre de données devant être utilisé pour fournir des services d'informatique en nuage;

b) [S'applique uniquement dans le cas du travail Protégé A et B et des modèles de prestation de services IaaS/PaaS/SaaS] indiquer les services d'informatique en nuage qui sont offerts à partir de l'extérieur du Canada, y compris tous les endroits où les données sont stockées et traitées et où l'entrepreneur gère le service à partir du Canada.

(5) L'entrepreneur des services d'informatique en nuage proposés a l'obligation continue de fournir un avis écrit au Canada lorsque des mises à jour sont apportées à la liste des emplacements physiques susceptibles de contenir des données du Canada.

11. Transfert et récupération des données

L'entrepreneur doit fournir la capacité, y compris les outils et les services, permettant au Canada d'effectuer ce qui suit :

a) Extraire toutes les données du Canada en ligne, près de la ligne 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'activité dans le nuage, le code source hébergé dans un dépôt de code du Canada et les configurations de réseau, de telle sorte que tout utilisateur final du Canada puisse utiliser ces instructions pour migrer d'un environnement à un autre environnement.

b) Transférer en toute sécurité toutes les données du Canada, y compris les données de contenu et les métadonnées associées, dans un format lisible et utilisable par machine, y compris le format CSV, et conformément aux lignes directrices de Bibliothèque et Archives Canada sur les formats de fichier pour le transfert des ressources d'information de valeur durable (Bibliothèque et Archives Canada).

12. Élimination des données et retour des documents au Canada

(1) L'entrepreneur doit éliminer ou réutiliser de façon sécuritaire les ressources (p. ex. équipement, stockage de données, fichiers et mémoire) qui contiennent les données du Canada et s'assurer que les données stockées antérieurement ne peuvent être consultées par d'autres clients après avoir été libérées. Cela comprend toutes les copies des données du Canada qui sont effectuées par

réplication à des fins de haute disponibilité et de reprise après sinistre. L'élimination ou la réutilisation des ressources par l'entrepreneur doit être conforme 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) Clearing and Declassifying Electronic Data Storage Devices (CSE ITSG-06). À la demande du Canada, l'entrepreneur doit fournir un document décrivant son processus d'élimination ou de réutilisation des ressources.

(2) L'entrepreneur doit fournir au Canada une confirmation écrite démontrant l'effacement, la purge ou la destruction réussie de toutes les ressources, selon le cas, et la capacité d'empêcher la réinstallation de tout système, capacité (logiciel ou processus), donnée ou instance d'information enlevée ou détruite une fois que le Canada cesse d'utiliser les services d'informatique en nuage.

13. Protection cryptographique

L'entrepreneur 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 VPN, TLS, modules logiciels, ICP et jetons d'authentification, le cas échéant), conformément aux algorithmes cryptographiques approuvés par le Centre de la sécurité des télécommunications (CST) et à la taille des paramètres cryptographiques, à la longueur des clés et aux périodes de cryptage des clés, comme il est spécifié dans les documents *Algorithmes cryptographiques pour l'information NON CLASSIFIÉ, PROTÉGÉ A et PROTÉGÉ B (ITSP.40.111)* et *Conseils sur la configuration sécurisée des protocoles réseau* (ITSP.40.062) et restent conformes à toute version ultérieure publiée dans le site web du Centre canadien pour la cybersécurité.

b) Utiliser des algorithmes cryptographiques approuvés par le CST et validés par le Cryptographic Algorithm Validation Program (CAVP), avec des tailles de paramètres cryptographiques et des longueurs clés, comme l'indique le document *Algorithmes cryptographiques pour l'information NON CLASSIFIÉ, PROTÉGÉ A et PROTÉGÉ B (ITSP.40.111)* et rester conforme à toute version ultérieure publiée dans le site web du Centre canadien pour la cybersécurité.

c) Veiller à ce que l'utilisation d'algorithmes cryptographiques, la taille des paramètres cryptographiques, la longueur des clés et les périodes cryptographiques soient configurables et puissent être mises à jour dans les protocoles, les applications et les services afin d'être conformes aux orientations en matière de transition à temps pour respecter les dates de transition spécifiées dans les documents *Algorithmes cryptographiques pour l'information NON CLASSIFIÉ, PROTÉGÉ A et PROTÉGÉ B (ITSP.40.111)* et *Conseils sur la configuration sécurisée des protocoles réseau* (ITSP.40.062) et rester conforme à toute version ultérieure publiée dans le site web du Centre canadien pour la cybersécurité. Les entrepreneurs doivent soutenir la transition vers une cryptographie à sécurité quantique, conformément aux orientations énoncées dans les documents ITSP.40.111 et ITSP.40.062 et dans leurs versions ultérieures.

d) Veiller à ce que des modules cryptographiques validés par le programme de validation des modules cryptographiques (PVMC) soient utilisés lorsque la cryptographie est nécessaire, et qu'ils soient mis en œuvre, configurés et exploités conformément à la politique de sécurité des modules cryptographiques figurant sur la liste des modules validés par le PVMC (NIST), dans un mode approuvé ou autorisé, afin de garantir avec un degré élevé de certitude que le module cryptographique validé par le PVMC fournit les services de sécurité attendus, de la façon prévue.

e) S'assurer que tous les modules cryptographiques utilisés disposent d'une certification active, en vigueur et valide en vertu du PVMC. Les produits validés par le biais du PVMC ont des numéros de certificat figurant sur la liste des modules validés par le biais du PVMC.

14. Gestion des clés

L'entrepreneur doit fournir au Canada un service de gestion des clés conforme au Guide sur le chiffrement des services infonuagiques (ITSP.50.106) et de toute version ultérieure publiée dans le site web du Centre canadien pour la cybersécurité, et prévoyant ce qui suit :

a) Capacité de créer/générer et de supprimer des clés de chiffrement si le GC l'exige.

b) Définition et application de politiques spécifiques pour contrôler la manière dont les clés peuvent être utilisées.

c) Protection de l'accès au matériel clé, y compris la prévention de l'accès de l'entrepreneur à l'information non chiffrée.

d) Possibilité d'effectuer un audit de tous les événements liés aux services de gestion des clés, y compris l'accès des entrepreneurs pour un examen par le GC.

e) Possibilité d'importer en toute sécurité des clés générées par le GC à partir d'un module de sécurité du matériel (HSM) sur place, géré par le GC, sans exposition du message en clair durant le processus d'importation.

f) La capacité d'empêcher le fournisseur de services d'informatique en nuage de récupérer des copies en clair des clés générées par le GC.

g) Possibilité de déléguer les privilèges d'utilisation des clés aux services d'informatique en nuage utilisés pour les services gérés par le GC.

15. Protection de l'équipement

L'entrepreneur doit mettre en œuvre, gérer et surveiller l'équipement renforcé sur le plan de la sécurité et doté de protections actives basées sur le système hôte afin de prévenir les logiciels malveillants, les attaques et les utilisations abusives, conformément aux lignes directrices de configuration reconnues par l'industrie, dont le *Guide to General*

Server Security (NIST 800-123), les Center for Internet Security (CIS) Benchmarks ou une norme équivalente approuvée par écrit par le Canada.

16. Développement sécurisé

L'entrepreneur doit mettre en œuvre un cycle de développement des logiciels et des systèmes axé sur 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 des logiciels, des sites web et des services, et qui est conforme aux normes de l'industrie et aux pratiques exemplaires comme (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 GC, l'entrepreneur doit fournir un document qui décrit l'approche et le processus documentés du cycle de vie du développement des logiciels et systèmes de l'entrepreneur.

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

(1) L'entrepreneur doit être en mesure, pour le Canada, d'assurer un accès sécurisé aux services d'informatique en nuage, y compris la capacité de les configurer :

a) Authentification multifactorielle résistante à l'hameçonnage, conformément au Guide sur l'authentification des utilisateurs dans les systèmes de technologie de l'information (ITSP.30.031 V3) du CCS (ou ses versions ultérieures), à l'aide de données d'identification approuvées par le GC.

b) Accès fondé sur les rôles

c) Contrôles de l'accès aux objets stockés

d) Politiques d'autorisation granulaires permettant d'autoriser ou de limiter l'accès.

(2) L'entrepreneur doit être en mesure d'établir des valeurs par défaut à l'échelle de l'organisation pour gérer les politiques applicables à l'ensemble des locataires.

18. Fédération

(1) L'entrepreneur doit être en mesure, pour le Canada, de prendre en charge l'intégration de l'identité fédérée, notamment :

a) La prise en charge de normes ouvertes pour les protocoles d'authentification tels que SAML (Security Assertion Markup Language) 2.0 (ou versions ultérieures) et OpenID Connect 1.0 (ou versions ultérieures), lorsque le contrôle des données d'identification de l'utilisateur final et l'authentification aux fins des services d'informatique en nuage relève exclusivement du Canada.

b) Possibilité d'associer des identifiants propres au Canada (par exemple, un code d'identification, une adresse électronique au Canada, etc.) au(x) compte(s) d'utilisateur(s) correspondant(s) du service en nuage.

19. Gestion de l'accès privilégié

(1) L'entrepreneur doit :

a) Mettre en œuvre des politiques et des procédures de contrôle d'accès axées sur l'intégration, la désinscription, la transition entre les rôles, l'examen périodique de l'accès pour identifier les privilèges excessifs, les limitations et le contrôle de l'utilisation des privilèges de l'administrateur.

b) Gérer et contrôler l'accès privilégié aux services d'informatique en nuage afin de garantir que toutes les interfaces de service dans un environnement à plusieurs locataires sont protégées contre les accès non autorisés, y compris celles qui sont utilisées pour héberger les services du GC.

c) Restreindre et minimiser l'accès aux services d'informatique en nuage et aux données au Canada aux seuls appareils et utilisateurs finaux ayant un besoin explicite d'y accéder.

d) Appliquer et vérifier les autorisations d'accès aux services d'informatique en nuage et aux données du Canada.

e) Limiter l'accès aux interfaces de services qui hébergent les données du Canada aux utilisateurs finaux, dispositifs et processus (ou services) identifiés, authentifiés et autorisés de façon unique.

f) Mettre en œuvre des politiques de mot de passe pour protéger les données d'identification contre les risques de compromission par des attaques en ligne ou hors ligne et pour détecter ces attaques en enregistrant et en surveillant des événements tels que (i) l'utilisation réussie des données d'identification, (ii) l'utilisation inhabituelle des données d'identification et (iii) l'accès à la base de données des mots de passe et son exfiltration, conformément au Guide sur l'authentification des utilisateurs dans les systèmes de technologie de l'information (ITSP.30.031 V3) du CCS (ou à ses versions ultérieures).

g) Mettre en œuvre des mécanismes d'authentification multifactorielle pour authentifier les utilisateurs finaux ayant un accès privilégié, conformément au Guide sur l'authentification des utilisateurs dans les systèmes de technologie de l'information (ITSP.30.031 V3) du CCS (ou à ses versions ultérieures).

h) Mettre en œuvre des mécanismes de contrôle d'accès fondés sur les rôles afin d'attribuer des privilèges qui constituent la base de l'application de l'accès aux données du Canada.

i) Définir et mettre en œuvre la séparation des tâches afin de séparer, à tout le moins, 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 des accès des autres rôles opérationnels.

j) Respecter les principes du moindre privilège et du besoin d'en connaître lorsqu'il s'agit d'accorder l'accès aux services d'informatique en nuage et aux données du Canada.

k) Utiliser des terminaux renforcés sur le plan de la sécurité (par exemple, des ordinateurs, des dispositifs d'utilisateur final, des serveurs de saut, etc.) qui sont configurés pour une fonctionnalité minimale (par exemple, un terminal dédié qui ne permet pas de naviguer sur Internet ou d'accéder au courriel) afin de fournir une assistance et une administration des services d'informatique en nuage et de l'infrastructure de l'entrepreneur.

l) Mettre en œuvre un processus automatisé pour vérifier périodiquement, à tout le moins, les mesures de création, de modification, d'activation, de désactivation et de suppression des comptes.

m) En cas de cessation d'emploi, résilier ou révoquer les codes d'authentification et les identifiants d'accès associés à tout membre du personnel des services.

(2) À la demande du Canada, l'entrepreneur doit fournir un document décrivant son approche et son processus de gestion et de surveillance de l'accès privilégié aux services d'informatique en nuage.

20. Gestion à distance

(1) L'entrepreneur doit gérer et surveiller l'administration à distance de son service d'informatique en nuage qui est utilisé pour héberger les services du GC et prendre des mesures raisonnables pour :

a) Mettre en œuvre des mécanismes d'authentification multifactorielle pour authentifier les utilisateurs d'accès à distance, conformément au Guide sur l'authentification des utilisateurs dans les systèmes de technologie de l'information (ITSP.30.031 V3) du CCS (ou à ses versions ultérieures).

b) Utiliser des mécanismes cryptographiques pour protéger la confidentialité des sessions d'accès à distance, conformément à l'article 13 (protection cryptographique).

c) Faire passer tous les accès à distance par des points de contrôle d'accès contrôlés, surveillés et audités.

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

e) Autoriser l'exécution à distance de commandes privilégiées et l'accès à distance à des données importantes pour la sécurité.

(2) À la demande du Canada, l'entrepreneur doit fournir 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 d'informatique en nuage.

21. Sécurité des réseaux et des communications

L'entrepreneur doit :

a) Permettre au Canada d'établir des connexions sécurisées avec les services d'informatique en nuage, notamment en assurant la protection des données en transit entre le Canada et le service en nuage 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, conformément aux Conseils sur la configuration sécurisée des protocoles réseau (ITSP.40.062) du CCS et aux Algorithmes cryptographiques pour l'information NON CLASSIFIÉ, PROTÉGÉ A et PROTÉGÉ B (ITSP.40.111) du CCS.

c) Utiliser des certificats correctement configurés dans les connexions TLS, conformément aux orientations du CCS.

d) Permettre au Canada de mettre en œuvre des contrôles d'accès au réseau et des règles de sécurité qui limitent l'accès aux ressources du Canada aux seuls dispositifs et emplacements de réseau autorisés.

22. Connexions dédiées

[S'applique uniquement dans le cas du travail Protégé B et du modèle de prestation de services IaaS] Dans le cas du modèle IaaS, l'entrepreneur doit permettre au GC d'établir une connectivité redondante privée avec les services d'informatique en nuage, c'est-à-dire :

a) Établir la connectivité soit directement dans le réseau étendu (WAN) du GC, soit par l'entremise du fournisseur de services d'échange dans le nuage du GC situé au 151 Front à Toronto et/ou au 625, boul. René Lévesque à Montréal, ou dans un endroit approuvé par le GC à l'intérieur des limites géographiques du Canada.

b) Permettre des services complets de sauvegarde et de reprise après sinistre grâce à des connexions redondantes au sein des centres de données des entrepreneurs et entre eux.

c) Les liens de connectivité physique sont optiques et fournissent un minimum de 10 Gbps avec la possibilité d'ajouter des liens supplémentaires qui fournissent jusqu'à 40 Gbps en agrégat, avec une connectivité optionnelle de 100 Gbps.

d) Prise en charge de la virtualisation et de la multilocation pour tous les composants du réseau.

e) Prise en charge des protocoles de routage dynamique (BGP) pour toutes les connexions.

f) Soutien des protocoles approuvés par le GC, tels que décrits dans les documents suivants :

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

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

23. Journalisation et audit

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

(2) L'entrepreneur doit permettre au Canada de gérer et de configurer de façon centralisée le contenu à saisir dans les dossiers de vérification à partir de multiples composantes (p. ex. réseau, données, stockage, calcul, etc.) des services d'informatique en nuage consommés par le Canada, afin de permettre au Canada d'effectuer la surveillance de la sécurité, la production de rapports, l'analyse, l'enquête et la mise en œuvre de mesures correctives, selon les besoins. Il s'agit notamment de la possibilité pour le Canada de faire ce qui suit :

   a) Enregistrer et détecter les événements d'audit tels que (i) les tentatives d'ouverture de 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, conformément au Guide sur la consignation d'événements.

   b) Enregistrer dans des journaux (ou des fichiers journaux) des événements d'audit synchronisés dans le temps et horodatés en temps universel coordonné (UTC) et protégés contre tout accès, modification ou suppression non autorisés pendant qu'ils sont en transit et au repos.

   c) Fournir des alertes en temps réel en cas d'échec de l'audit au personnel habilité à y remédier.

   d) Enregistrer des incidents de sécurité et des journaux distincts pour différents comptes du Canada afin de permettre au Canada de surveiller et de gérer les

événements à l'intérieur de ses limites qui affectent son instance d'un service en nuage IaaS, PaaS ou SaaS qui lui est fourni par l'entrepreneur ou un sous-traitant.

(3) L'entrepreneur doit permettre au Canada d'exporter des événements et des journaux de sécurité à l'aide d'interfaces, de protocoles et de formats de données normalisés (p. ex. Common Event Format (CEF), syslog ou d'autres formats de journaux courants) et d'API qui permettent la récupération à distance des données de journaux (notamment par l'intermédiaire d'une interface de base de données utilisant le langage SQL, etc.) pour les services d'informatique en nuage utilisés à l'appui des opérations du GC, notamment la surveillance des services d'informatique en nuage, l'investigation informatique la mise en suspens juridique.

(4) Dans le cas du SaaS, l'entrepreneur doit fournir des API permettant ce qui suit :

i. [S'applique uniquement dans le cas du travail Non classifié, Protégé A et Protégé B et du modèle de prestation de services SaaS] Inspecter et interroger les données au repos dans les applications SaaS.

ii. [S'applique uniquement dans le cas du travail Non classifié, Protégé A et Protégé B et du modèle de prestations de services SaaS] Évaluer les événements tels que l'accès et le comportement des utilisateurs, l'accès et le comportement des administrateurs, ainsi que les modifications de l'accès aux API tierces, stockés dans les journaux des applications SaaS.

24. Surveillance continue

(1) L'entrepreneur doit continuellement gérer, surveiller et maintenir le niveau de sécurité de son infrastructure et des emplacements de services qui hébergent les données du Canada tout au long du contrat, et s'assurer que les services d'informatique en nuage fournis au Canada le sont d'une manière qui respecte les présentes obligations en matière de sécurité. Dans le cadre de ces obligations, l'entrepreneur doit :

a) Surveiller activement et continuellement les menaces et les vulnérabilités qui pèsent sur l'infrastructure de l'entrepreneur, les sites de services ou les données du Canada.

b) Procéder régulièrement à des analyses de vulnérabilité et à des tests de pénétration de l'infrastructure de l'entrepreneur et des sites de services, afin de déceler les lacunes et de les combler pour empêcher l'accès non autorisé à des renseignements sensibles, le contournement des contrôles d'accès et l'escalade des privilèges, ainsi que l'exploitation des vulnérabilités pour accéder à des systèmes ou à des renseignements.

c) S'efforcer de prévenir les attaques grâce à des mesures de sécurité telles que des mesures de protection contre les dénis de service.

d) Faire tout en son possible pour détecter les attaques, les incidents de sécurité et d'autres événements anormaux.

e) Déceler l'utilisation et l'accès non autorisés à tout service d'informatique en nuage, à toute donnée et à tout composant pertinent au service d'informatique en nuage IaaS, PaaS ou SaaS du Canada.

f) 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 remédier à tout problème signalé publiquement dans les services d'informatique en nuage ou les bibliothèques que les services d'informatique en nuage utilisent, et fournir des avis préalables sur les correctifs conformément aux engagements convenus en matière de niveau de service.

g) Répondre aux menaces et attaques contre les services d'informatique en nuage de l'entrepreneur, contenir celles-ci et assurer la reprise des activités.

h) Prendre au besoin des contre-mesures proactives, notamment des mesures préventives et réactives, pour atténuer les menaces.

(2) Les services d'informatique en nuage de l'entrepreneur doivent permettre de copier et d'acheminer à un endroit prédéterminé (dans l'informatique en nuage ou dans les locaux du GC) les données des applications du GC (pour les modèles de prestation de services IaaS, PaaS et SaaS) et le trafic réseau du GC (pour les modèles de prestation de services IaaS et PaaS) des services du GC hébergés dans l'informatique en nuage.

Remarque à l'intention de l'autorité contractante : Choisissez votre méthode de prestation de services d'informatique en nuage dans la section 24.3, en fonction de vos besoins.

(3) *Dans le cas des modèles de prestation de services IaaS/PaaS, les services d'informatique en nuage de l'entrepreneur doivent permettre au Canada de déployer et d'exploiter un logiciel de sécurité pour effectuer une surveillance avancée et des mesures d'atténuation des cybermenaces pour les services d'informatique en nuage du Canada au niveau de l'hôte et du réseau gérés par le Canada, pour les composantes gérées par le Canada seulement.*

ou

Dans le cas du modèle de prestation de services SaaS, les services d'informatique en nuage de l'entrepreneur doivent permettre au Canada de déployer et d'exploiter un logiciel de sécurité pour effectuer une surveillance avancée et des mesures d'atténuation des cybermenaces pour les services d'informatique en nuage du Canada pour les composantes gérées par le Canada seulement.

25. Gestion des incidents de sécurité

(1) Le processus de réponse aux incidents de sécurité de l'entrepreneur en ce qui concerne les services d'informatique en nuage doit englober le cycle de vie de la

gestion des incidents de sécurité informatique et les pratiques de soutien pour les activités de préparation, de détection, d'analyse, d'endiguement et de reprise des activités, c'est-à-dire :

a) Un processus de réponse aux incidents de sécurité publié et documenté, soumis à l'examen du Canada, qui est conforme à l'une des normes suivantes : (i) ISO/IEC 26035 : 2011 Technologies de l'information – Techniques de sécurité – Gestion des incidents de sécurité de l'information, (ii) NIST SP800-612, Computer Security Incident Handling Guide, (iii) Plan de gestion des événements de cybersécurité du gouvernement du Canada (PGEC GC) ou (iv) d'autres normes de l'industrie si le Canada estime que celles-ci répondent à ses exigences en matière de sécurité.

b) Processus et procédures documentés quant à la façon dont l'entrepreneur identifiera les incidents de sécurité, y répondra, y remédiera, les signalera et les transmettra au Canada, y compris (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 des réponses connexes; (iii) le délai cible prévu pour la 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 questions relatives aux incidents liés à la sécurité de l'information, conformément aux procédures de notification énoncées dans le PGEC GC, et (vi) tout recours applicable en cas d'incidents liés à la sécurité de l'information.

c) La capacité de l'entrepreneur à soutenir les efforts d'enquête du Canada pour toute compromission décelée dans le cas des utilisateurs ou des données.

d) Seuls les représentants désignés et préautorisés du client (p ex., le Centre canadien pour la cybersécurité et d'autres organisations approuvées par le GC) et autorisés par le responsable technique peuvent :

    (i) demander et recevoir un accès discret et de l'information relative aux données du client (données de l'utilisateur, journaux d'événements du système/de la sécurité, captures de paquets du réseau ou de l'hôte, journaux des composants de sécurité tels que IDS/IPS/Firewalls, etc.) de façon non chiffrée, afin de mener des enquêtes;
    (ii) suivre l'état d'un événement signalé en matière de sécurité de l'information;

e) Procédures pour répondre aux demandes de preuves numériques potentielles ou d'autres données provenant de l'environnement des services d'informatique en nuage et conformes aux normes et aux meilleures pratiques du secteur, notamment la norme ISO 22095 : 2020 Chaîne de contrôle – Terminologie générale et modèles), y compris les procédures médico-légales et les mesures de protection appropriées pour :

    (i) le maintien d'une chaîne de contrôle pour les données d'audit;

(ii) la collecte, la conservation et la présentation de preuves qui démontrent l'intégrité de ces dernières.

(2) Dans les 10 jours suivant la date d'entrée en vigueur du contrat, l'entrepreneur doit fournir un document décrivant sa procédure de réponse aux incidents de sécurité, y compris les coordonnées des personnes à contacter. Ce processus, y compris les coordonnées, doit rester à jour et, au minimum, être validé sur une base annuelle et approuvé par le Canada.

(3) L'entrepreneur doit :

a) Collaborer avec les centres des opérations de sécurité du Canada (p. ex. le COS du GC, les équipes ministérielles de sécurité des TI) et les principaux intervenants du PGEC (c.-à-d. le CCS et le Secrétariat du Conseil du Trésor du Canada (SCT)) en ce qui a trait à l'endiguement, l'éradication et la reprise des activités en cas d'incidents de sécurité, conformément au Plan de gestion des événements de cybersécurité du gouvernement du Canada (PGEC GC).

b) Conserver un registre des violations de sécurité avec une description de la violation, la période de temps, les conséquences de la violation, le nom du déclarant, et à qui la violation a été signalée, la procédure de récupération des données ou du service, et les enregistrements des activités liées à la gestion de l'incident de sécurité, y compris les communications internes et externes (notamment dans le cas d'un rançongiciel, toutes les communications, y compris les demandes de rançon, etc.). Ces données doivent être fournies au Canada sur demande.

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

(4) Pour appuyer les enquêtes de sécurité, le Canada peut exiger de l'entrepreneur des preuves médico-légales pour l'aider dans une enquête du GC. L'entrepreneur doit :

a) conserver les rapports d'enquête relatifs à une enquête de sécurité pendant une période de deux ans après la fin de l'enquête ou les fournir au Canada pour qu'ils soient conservés;

b) fournir un soutien raisonnable en matière d'enquête aux représentants désignés et préautorisés du Canada, tels que le CCS et la Gendarmerie royale du Canada (GRC);

c) maintenir la chaîne de contrôle des preuves conformément aux meilleures pratiques telles que celles décrites dans la norme ISO 22095:2020;

d) soutenir l'investigation électronique;

e) conserver les dossiers juridiques pour répondre aux besoins dans le cas des enquêtes et des demandes judiciaires.

(5) Si l'entrepreneur fait appel à une entreprise externe pour ses activités de réponse aux incidents, il est tenu de veiller à ce que les dispositions énoncées à l'*article 25 – Gestion des incidents de sécurité* et à l'*article 26 – Réponse aux incidents de sécurité* s'appliquent également à l'équipe externe de réponse aux incidents et soient documentées dans le cadre du processus de réponse aux incidents de sécurité de l'entrepreneur.

26. Réponse aux incidents de sécurité

(1) L'entrepreneur doit alerter et aviser promptement le Canada (par téléphone et par courriel), conformément aux dispositions de l'article 25, en cas de compromission, de violation ou de tout élément de preuve tel que (i) un incident de sécurité, (ii) une défaillance de sécurité dans le cas d'un bien, (iii) un accès irrégulier ou non autorisé à un bien, (iv) la copie à grande échelle d'un document d'information ou (v) toute autre activité irrégulière identifiée par l'entrepreneur, qui l'amène à penser raisonnablement qu'un risque de compromission ou une atteinte à la sécurité ou à la vie privée est ou peut être imminent, ou que 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 effectuée sans retard excessif, en tout état de cause dans les 72 heures, et dans le respect des engagements pris par l'entrepreneur en matière de niveau de service.

(2) Si l'entrepreneur prend connaissance d'une compromission ou d'une violation de la sécurité menant à la destruction, à la perte, à l'altération, à la divulgation non autorisée ou à l'accès accidentel ou illégal aux données sur les clients ou aux renseignements personnels pendant qu'ils sont traités par l'entrepreneur (un « incident de sécurité » dans chaque cas), l'entrepreneur doit promptement et sans retard injustifié (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 les mesures nécessaires pour atténuer la cause de l'incident et minimiser tout dommage résultant de l'incident de sécurité.

(3) Les entrepreneurs sont tenus de signaler les incidents majeurs au service de police compétent lorsque le Canada le demande.

27. Fuite de données

(1) L'entrepreneur doit disposer d'un processus documenté décrivant l'approche à suivre en cas d'incident lié à une fuite de données. Le processus en question doit s'aligner sur : (i) la norme ITSG-33 Security Control for IR-9 Information Spill Response ou (ii) une autre norme industrielle, approuvée par écrit par le Canada. Nonobstant ce qui précède, le processus de l'entrepreneur décrivant l'approche à adopter en cas de fuite de données doit prévoir, à tout le moins :

a) Un processus d'identification des éléments d'information visés en cas de contamination d'un système.

b) Un processus permettant d'isoler et d'éradiquer un système contaminé.

c) Un processus d'identification des systèmes susceptibles d'avoir été

contaminés par la suite et toute autre mesure prise pour éviter une nouvelle contamination.

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

28. Vérification et validation de la sécurité

(1) L'entrepreneur doit disposer d'un processus permettant d'effectuer une analyse de vulnérabilité ou un test de pénétration non perturbateur et non destructeur des services d'informatique en nuage hébergeant les données du Canada. Cela inclut la capacité d'effectuer des analyses internes et externes périodiques se rapportant à la location du GC et, lorsque des changements importants sont apportés à la plateforme principale, à identifier toute vulnérabilité potentielle du système liée à la location du GC en procédant à :

i. des analyses de vulnérabilité;
ii. des analyses d'applications web;
iii. des tests de pénétration.

(2) L'entrepreneur doit élaborer un plan d'action et des étapes déterminantes pour documenter toutes les mesures correctives prévues afin de remédier aux faiblesses ou de combler les lacunes de la plateforme principale et ainsi réduire ou éliminer les vulnérabilités connues du système, ou celles qui pourraient être liées aux services d'informatique en nuage qui hébergent les données du Canada et à l'exploitation de la location du GC.

(3) À la demande du Canada, l'entrepreneur doit fournir les résultats de la mise à l'essai de l'ensemble de la plateforme, ainsi que le plan d'action et la documentation sur les étapes à franchir à des fins de planification et d'examen.

(4) [S'applique uniquement dans le cas du travail Protégé A et Protégé B et du modèle de prestation de services IaaS] 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 de la partie canadienne des composantes du service d'informatique en nuage dans l'environnement de l'entrepreneur.

(5) L'entrepreneur doit fournir la capacité d'activer un bilan de sécurité en libre-service ou un outil de notation permettant mesurer la posture de sécurité des services d'informatique en nuage configurés par le Canada.

29. Enquête de sécurité sur le personnel

(1) L'entrepreneur doit mettre en œuvre des mesures de sécurité qui accordent et maintiennent le niveau requis d'habilitation de sécurité pour ses employés affectés à la prestation de services d'informatique en nuage et pour les employés des sous-traitants, conformément à leurs privilèges d'accès aux actifs des systèmes d'information dans lesquels les données du Canada sont stockées et traitées.

(2) Les mesures de filtrage de sécurité du personnel de l'entrepreneur doivent être appliquées conformément à la définition et aux pratiques de la Norme sur le filtrage de sécurité du Conseil du Trésor ou conformément à un équivalent acceptable approuvé par le Canada.

(3) À la demande du Canada, l'entrepreneur doit fournir un document décrivant son processus d'enquête de sécurité sur le personnel. Ce processus doit prévoir, à tout le moins :

a) Une description des postes d'employés et de sous-traitants qui nécessitent un accès aux données du client ou qui ont la capacité d'affecter la confidentialité, l'intégrité ou la disponibilité des services d'informatique en nuage.

b) Une description des activités et des pratiques en matière d'enquêtes de sécurité, y compris les procédures de notification à suivre si l'enquête n'est pas terminée ou si les résultats suscitent des doutes ou des inquiétudes.

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 manière continue, afin de garantir que les employés et les sous-traitants comprennent leurs responsabilités en matière de sécurité de l'information, en soient conscients et les assument.

d) Une description de la procédure mise en œuvre lorsqu'un employé ou un sous-traitant change de rôle ou lorsque son emploi prend fin.

e) L'approche adoptée pour détecter les menaces internes potentielles, y répondre et les atténuer, ainsi que les contrôles de sécurité mis en œuvre pour atténuer le risque d'accès aux données du GC et/ou l'incidence sur la fiabilité des services d'informatique en nuage qui hébergent les données du Canada.

30. Sécurité matérielle (centre de données/installations)

(1) L'entrepreneur doit mettre en œuvre des mesures de sécurité matérielle pour assurer la protection des installations informatiques et des actifs des systèmes d'information dans lesquels les données du Canada sont stockées et traitées contre toute forme d'altération, de perte, de dommage et de saisie. La protection physique de toutes les installations qui hébergent des données du Canada doit être appliquée conformément à une approche adéquate fondée sur le risque et basée sur une approche de sécurité matérielle de type « prévention-détection-intervention-rétablissement », alignée sur les contrôles de sécurité matérielle et les pratiques énoncées dans la Norme opérationnelle sur la sécurité matérielle du Conseil du Trésor, ou utiliser une approche adéquate fondée sur le risque. Les mesures de sécurité exigées en vertu de cette disposition comprennent, à tout le moins :

(i) Des capacités de redondance et de rétablissement suffisantes, dans le cas des installations de l'entrepreneur et entre celles-ci, y compris une disparité géographique telle que la perte d'une installation n'empêche pas

la récupération des données et des données du Canada dans le respect des engagements prescrits en matière de niveau de service.

(ii) Un traitement approprié des supports informatiques.

(iii) La maintenance contrôlée de tous les systèmes d'information et de leurs composants afin de protéger leur intégrité et d'assurer leur disponibilité permanente.

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

(v) Des mesures pour permettre l'accès physique aux emplacements des données et des services du Canada uniquement au personnel autorisé affecté aux services d'informatique en nuage, en fonction du poste ou du rôle et du principe de nécessité d'accès, et validé par deux formes d'identification.

(vi) L'accompagnement des visiteurs et un contrôle de leurs activités.

(vii) Des mesures de sauvegarde pour les données du GC sur des sites de travail alternatifs (par exemple, des sites de télétravail).

(viii) L'enregistrement et la surveillance de tous les accès physiques aux points de service et de tous les accès logiques aux systèmes hébergeant les données du Canada, à l'aide d'une combinaison de registres d'accès, de système de vidéosurveillance dans toutes les zones sensibles et de mécanismes de détection des intrusions.

(ix) Des contrôles de sécurité continus sur les lieux de service et dans les installations afin de détecter toute exfiltration non autorisée de données ou de composants du système.

(2) À la demande du Canada, l'entrepreneur doit fournir un document décrivant ses mesures de sécurité matérielle.

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

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

(1) L'entrepreneur doit mettre en œuvre des mesures de protection pour atténuer les menaces et les vulnérabilités de la chaîne d'approvisionnement des services informatiques afin de maintenir la confiance dans la sécurité des sources des systèmes d'information et des composants informatiques utilisés pour fournir des services d'informatique en nuage. Cela comprend, sans s'y limiter, la protection

tout au long du cycle de développement des systèmes par 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 basé sur les rôles et un droit d'accès minimal pour l'ensemble du personnel de la chaîne d'approvisionnement; la sensibilisation aux menaces, la formation du personnel chargé des acquisitions en ce qui a trait aux menaces, aux risques et aux contrôles de sécurité requis; et l'obligation, pour les entités de la chaîne d'approvisionnement, de mettre en œuvre les mesures de protection nécessaires.

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

(i) ISO/IEC 27036 Technologies de l'information – Techniques de sécurité – Relations 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) ITSG-33 security control for SA-12 where the organization defined security safeguards are documented in an SRCM plan.

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

a) Fournir la preuve que l'approche et le plan SRCM ont été évalués et validés par un tiers indépendant certifié par l'AICPA ou CPA Canada, et/ou par le régime de certification ISO

OU

b) Fournir au Canada une copie du plan SRCM chaque année ou à la demande du Canada.

(4) [S'applique uniquement dans le cas du modèle de prestation de services SaaS] Lorsque l'entrepreneur est un fournisseur de SaaS utilisant un fournisseur IaaS approuvé par le GC 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 doit fournir à l'entrepreneur approuvé par le GC une liste de produits de technologies de l'information et de la communication (TIC) décrivant l'équipement TIC déployé dans l'environnement du fournisseur de services Internet approuvé par le GC en vue d'un examen de l'intégrité de la chaîne d'approvisionnement (SCSI). Cet examen sera effectué tous les trois ans.

32. Sous-traitants

(1) L'entrepreneur doit fournir une liste des sous-traitants auxquels il pourrait confier toute partie des travaux dans le cadre de la fourniture du contrat attribué par le Canada. Cette liste doit renfermer les données suivantes : (i) le nom des sous-traitants; (ii) la nature des travaux qui seront effectués par les sous-traitants; (iii) le(s) lieu(x) où les sous-traitants effectueront ces travaux.

(2) L'entrepreneur doit fournir une liste des sous-traitants dans les 10 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'être informé de cette mise à jour) de tout nouveau sous-traitant au moins 14 jours avant de lui donner accès aux données du client ou aux données à caractère personnel. Le fournisseur doit aider le Canada à vérifier les sous-traitants dans un délai de 10 jours ouvrables.

33. Programme de la sécurité industrielle – Exigences en matière de sécurité dans le cas des fournisseurs canadiens

(1) [S'applique uniquement dans le cas du travail Protégé A et Protégé B] L'entrepreneur ou le soumissionnaire doit, en tout temps pendant l'exécution du contrat, de l'offre à commandes ou de l'arrangement en matière d'approvisionnement, détenir une vérification d'organisation désignée (VOD) valide et une autorisation de détenir des documents de niveau PROTÉGÉ A ou B (le cas échéant), émise par le Programme de sécurité des contrats (PSC) de Services publics et Approvisionnement Canada (SPAC).

(2) Chacun des membres du personnel de l'entrepreneur/du soumissionnaire devant avoir accès aux données, aux biens ou au(x) site(s) de travail PROTÉGÉS doit détenir une habilitation de sécurité valide au niveau SECRET, ou une COTE DE FIABILITÉ, accordée ou approuvée par le PSC de SPAC.

(3) L'entrepreneure NE DOIT PAS utiliser ses systèmes informatiques pour traiter, produire ou stocker électroniquement des renseignements PROTÉGÉS avant d'avoir obtenu l'autorisation écrite du responsable de la sécurité du ministère client. Une fois cette autorisation accordée, ces tâches peuvent être exécutées au niveau PROTÉGÉ A ou B (le cas échéant), y compris un lien informatique au niveau PROTÉGÉ A ou B (le cas échéant).

(4) Les contrats de sous-traitance renfermant des exigences en matière de sécurité ne doivent PAS être attribués sans l'autorisation écrite préalable du PSC de SPAC.

(5) L'entrepreneur ou le soumissionnaire doit se conformer aux dispositions des documents suivants :

a) Liste de vérification des exigences relatives à la sécurité et guide de sécurité (le cas échéant) – annexes B et C.

b) [S'applique uniquement dans le cas du travail Protégé A et Protégé B] Manuel de la sécurité des contrats (version la plus récente).

c) [S'applique uniquement dans le cas du travail Protégé A et Protégé B] Exigences de sécurité des contrats du gouvernement du Canada

REMARQUE : Ce dossier comporte plusieurs niveaux d'enquêtes de sécurité sur le personnel. Dans ce cas, un guide de sécurité doit être ajouté à la Liste de vérification des exigences relatives à la sécurité pour clarifier ces contrôles. Le guide de sécurité est

normalement établi par le responsable du projet et/ou le responsable de la sécurité.

34. Programme de la sécurité industrielle – Exigences en matière de sécurité dans le cas des fournisseurs étrangers

[S'applique uniquement dans le cas du travail Protégé A et Protégé B] L'autorité canadienne désignée en matière de sécurité (ACDS) pour les questions de sécurité industrielle au Canada est le Secteur de la sécurité industrielle (SSI) de Services publics et Approvisionnement Canada (SPAC), et relève de la Direction de la sécurité industrielle internationale (DSII) de ce ministère. L'ACDS est responsable de la vérification du respect, par l'**entrepreneur** ou le **sous-traitant,** des exigences en matière de sécurité applicables aux fournisseurs étrangers. Les exigences ci-après s'appliquent aux **entrepreneurs et sous-traitants** étrangers constitués en société ou autorisés à faire des affaires dans une juridiction autre que le Canada et fournissant/exécutant à l'extérieur du Canada les services d'informatique nuage décrits dans la solution en nuage, en plus des exigences en matière de confidentialité et de sécurité. Ces exigences en matière de sécurité s'ajoutent aux exigences indiquées dans la section intitulée Protection et sécurité des données stockées dans les bases de données.

(1) L'**entrepreneur ou le sous-traitant** certifie que la livraison et la prestation de services d'informatique en nuage en vertu du présent contrat doivent 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 un instrument de sécurité bilatéral international. Le Programme de sécurité des contrats (PSC) dispose d'instruments de sécurité bilatéraux internationaux conclus avec la liste des pays incluse dans le site web de SPAC : http://www.tpsgc-pwgsc.gc.ca/esc-src/international-fr.html, mise à jour à l'occasion.

(2) L'**entrepreneur ou le sous-traitant** étranger doit, à tout moment pendant l'exécution du **contrat/de la sous-traitance**, être enregistré auprès de l'autorité de contrôle gouvernementale appropriée dans le(s) pays où il est constitué ou exerce ses activités et où il est autorisé à faire des affaires. L'**entrepreneur ou le sous-traitant** étranger doit fournir à l'autorité contractante et à l'ACDS la preuve de son enregistrement auprès de l'autorité de contrôle compétente.

(3) L'**entrepreneur ou le sous-traitant** étranger doit fournir la preuve qu'il est constitué en société ou autorisé à faire des affaires dans son pays.

(4) L'entrepreneur étranger ne doit pas commencer les travaux, les services ou les prestations avant que l'ACDS ne se soit assurée que toutes les conditions relatives aux exigences de sécurité du contrat ont été remplies. La confirmation de l'ACDS doit être fournie, par écrit, à l'entrepreneur étranger dans un formulaire de certification, afin de confirmer la conformité et l'autorisation des services à fournir.

(5) L'**entrepreneur ou le sous-traitant** étranger doit désigner un responsable de la sécurité du contrat autorisé et un responsable suppléant (le cas échéant) qui seront chargés de superviser les exigences en matière de sécurité définies dans le présent contrat. Cette personne sera nommée par le promoteur, le chef de la

direction de **l'entrepreneur ou du sous-traitant** étranger ou un haut fonctionnaire clé désigné, défini comme un responsable, un dirigeant, un administrateur, un cadre ou un partenaire occupant un poste qui lui permettrait d'influer négativement sur les politiques ou les pratiques de l'organisation dans le cadre de l'exécution du contrat.

(6) L'**entrepreneur ou le sous-traitant** ne doit pas accorder l'accès aux données/biens du Canada **PROTÉGÉ B**, sauf pour ce qui est du personnel ayant besoin d'y accéder pour l'exécution du **contrat** et qui a fait l'objet d'une enquête conformément à la définition et aux pratiques de la Norme sur le filtrage de sécurité du Conseil du Trésor ou utiliser des mesures équivalentes acceptables approuvées par le Canada.

(7) Les données/biens **PROTÉGÉS du CANADA** fournis à un **entrepreneur ou un sous-traitant** étranger, ou produits par un **entrepreneur ou sous-traitant** étranger :

i. ne peuvent être divulgués à un autre gouvernement, à une autre personne ou entreprise, ou à un représentant de ceux-ci, qui ne sont pas directement liés à l'exécution du **contrat**, sans le consentement écrit préalable du Canada. Ce consentement doit être demandé à l'ACDS, en collaboration avec l'autorité contractante; et

ii. ne peuvent être utilisés à d'autres fins que l'exécution du **contrat** sans l'approbation écrite préalable du Canada. Cette approbation doit être obtenue en contactant l'autorité contractante (en collaboration avec l'ADSC).

(8) L'**entrepreneur ou le sous-traitant** étranger NE DOIT PAS retirer les données/biens **PROTÉGÉS du CANADA** du ou des lieux de travail prévus, et l'**entrepreneur ou le sous-traitant** étranger doit s'assurer que les membres de son personnel sont au courant de cette restriction et qu'ils s'y conforment.

(9) L'**entrepreneur ou le sous-traitant** étranger ne doit pas utiliser les données/biens **PROTÉGÉS du CANADA** à des fins autres que l'exécution du **contrat** sans l'approbation écrite préalable du gouvernement du Canada. Cette approbation doit être obtenue auprès de l'ADSC.

(10) L'**entrepreneur ou le sous-traitant** étranger doit, à tout moment pendant l'exécution du **contrat**, détenir l'équivalent d'une autorisation de détenir des renseignements (ADR) de niveau **PROTÉGÉ B**.

(11) L'entrepreneur étranger doit immédiatement signaler à l'ADSC tous les cas où il a des raisons de croire que des données/biens PROTÉGÉS du CANADA dans le cadre du présent contrat ont été compromis.

(12) L'entrepreneur étranger doit assurer, dans le cas des données/biens PROTÉGÉS du CANADA, un niveau de protection non moins rigoureux que celui assuré par le gouvernement du Canada, conformément aux politiques nationales, à la législation et à la réglementation en matière de sécurité

nationale, ainsi qu'aux normes prescrites par l'ADSC.

(13) Une fois les travaux terminés, l'entrepreneur étranger doit retourner au gouvernement du Canada tous les biens et données PROTÉGÉS du CANADA fournis ou produits en vertu du présent contrat, y compris tous ceux qui ont été communiqués ou transmis à ses sous-traitants ou produits par ces derniers. L'entrepreneur étranger qui a besoin d'accéder à des données/biens PROTÉGÉS du CANADA ou à des sites canadiens à accès restreint, dans le cadre de ce contrat, doit soumettre une demande d'accès au responsable de la sécurité du ministère/de l'organisation visé(e) au Canada.

(14) L'entrepreneur étranger NE DOIT PAS utiliser ses systèmes de technologie de l'information (TI) pour traiter, produire ou stocker électroniquement sur un système informatique et transférer via une liaison TI des renseignements PROTÉGÉ B du Canada tant que l'autorisation de le faire n'a pas été confirmée par l'ADSC.

(15) Les contrats de sous-traitance qui contiennent des exigences en matière de sécurité ne doivent PAS être attribués sans une autorisation écrite préalable de l'ADSC canadienne.

(16) Les contrats attribués à un sous-traitant étranger tiers NE DOIVENT PAS être attribués sans l'autorisation écrite préalable de l'ADSC afin de confirmer les exigences de sécurité à imposer aux sous-traitants.

(17) Les contrats de sous-traitance attribués à un sous-traitant étranger tiers NE DOIVENT PAS être attribués sans l'autorisation écrite préalable de l'ADSC afin de confirmer les exigences de sécurité à imposer aux sous-traitants.

(18) L'**entrepreneur ou le sous-traitant** étranger doit se conformer aux dispositions de la liste de contrôle des exigences de sécurité jointe aux annexes B et C.

(19) Nonobstant tout article des conditions générales relative à la sous-traitance, l'entrepreneur étranger ne doit pas confier en sous-traitance (notamment à une société affiliée) une fonction qui implique de fournir à un sous-traitant l'accès à toute donnée relative au contrat, à moins que l'autorité contractante (en collaboration avec l'ADSC) n'y consente par écrit au préalable.

(20) Le Canada a le droit de rejeter toute demande présentée séparément et indépendamment de l'autorisation prévue dans le présent contrat relativement à la prestation de services d'informatique en nuage par l'entrepreneur pour accéder électroniquement aux données **PROTÉGÉES du CANADA** liées aux services d'informatique en nuage, les traiter, les produire, les transmettre ou les stocker dans tout autre pays s'il y a des raisons de s'inquiéter de la sécurité, de la protection des renseignements personnels ou de l'intégrité de l'information.

Remarque à l'intention de l'autorité contractante : L'article 35, Transport physique et transmission de données est une décision commerciale et donc une clause facultative pour l'utilisation des services de dispositifs de transfert de données.

35. Transport physique et transmission de données

(1) L'entrepreneur doit mettre en œuvre des mesures pour protéger les données matérielles du Canada, y compris les biens au repos (par exemple, en cours d'utilisation ou en entreposage), en transit (par exemple, en cours de transport ou de transmission) et par une destruction appropriée, c'est-à-dire qu'il doit :

a) Veiller à ce que les dispositifs de stockage de données portables soient correctement sécurisés à tout moment, en fonction du niveau le plus élevé de classification de sécurité des données qui y sont stockées, dans un conteneur de sécurité approprié, comme le prévoient le Manuel de la sécurité industrielle de SPAC, chapitre 5 (Manipulation et sauvegarde des renseignements et des biens classifiés et protégés) et chapitre 8 (Sécurité de la technologie de l'information), ainsi que les principes énoncés dans le Guide d'équipement de sécurité (G1-001) de la GRC, et à ce que le conteneur de sécurité soit protégé par un mot de passe et des mécanismes d'authentification solides.

b) Chiffrer toutes les données du Canada stockées sur des dispositifs de stockage de données portables à l'aide d'un module de chiffrement certifié par le Programme de validation des modules cryptographiques, et conformément à l'article 13 – Protection cryptographique, y compris l'utilisation de produits accrédités par le programme canadien lié aux critères communs.

c) Veiller à ce que, avant de connecter l'appareil au réseau informatique du Canada en vue de transferts unilatéraux de données des réseaux informatiques du Canada vers l'appareil, ce dernier fasse l'objet d'une recherche de logiciels malveillants à chaque fois qu'il est connecté à l'infrastructure informatique du Canada.

d) Veiller à ce que tous les dispositifs portables utilisés pour le transfert des données du Canada soient nettoyés afin d'empêcher la récupération des données, conformément aux exigences de nettoyage des supports décrites au paragraphe 12(1) - Élimination des données et retour des documents au Canada.

(2) Les renseignements protégés sont « en voie de transmission » jusqu'à ce qu'ils aient atteint leur destination et aient été livrés au centre de données de l'entrepreneur ou ouverts. S'ils sont ouverts, ils doivent alors être protégés, conformément à l'article 30 – Sécurité matérielle, et au Manuel de la sécurité industrielle de SPAC, chapitre 5 (Manipulation et sauvegarde des renseignements et des biens classifiés et protégés et chapitre 8 (Sécurité de la technologie de l'information).

(3) L'entrepreneur doit signaler toute perte ou tout vol réel ou soupçonné de dispositifs de stockage de données portables, conformément à l'article 26 – Réponse aux incidents de sécurité, et au Manuel de la sécurité industrielle de SPAC, chapitre 5 (Manipulation et sauvegarde des renseignements et des biens classifiés et protégés) et chapitre 8 (Sécurité de la technologie de l'information).