Annexe C- Appendice A - Guide de classification de la sécurité

Objectif

L'objet du présent document est de présenter les exigences en matière de contrôle de sécurité pour prendre en charge les rôles attendus et l'accès aux données du GC dans le contexte des services commerciaux infonuagiques.

Contexte

Conformément aux résultats attendus décrits à la section 5.2.2 de la *Norme sur le filtrage de sécurité* du Conseil du Trésor, les pratiques de filtrage de sécurité doivent fournir l'assurance raisonnable que l'on peut faire confiance aux personnes pour protéger les renseignements, les biens et les installations du gouvernement et pour s'acquitter de leurs fonctions de façon fiable. L'accès aux données du GC nécessite une autorisation ou une cote de sécurité valide. À ce titre, les exigences de sécurité incluent la limitation de l'accès aux seuls utilisateurs autorisés qui ont fait l'objet d'une enquête de sécurité au niveau approprié et qui ont besoin de savoir. Ces mesures s'étendent au personnel du fournisseur de services d'informatique en nuage[1] (FSI), qui, de par sa position, pourrait :

- obtenir un accès non autorisé aux données du GC;
- avoir la capacité de nuire aux services infonuagiques du GC;
- causer un préjudice à la réputation du GC.

Afin d'exercer leurs fonctions au nom du GC, les FSI doivent en tout temps démontrer les mesures qu'ils prennent pour accorder et maintenir le niveau de sécurité requis en vertu du processus de filtrage de sécurité pour leur personnel en fonction de leurs privilèges d'accès aux renseignements protégés. Dans tous les cas, l'accès à l'information, aux biens, aux installations ou aux systèmes de technologie de l'information (TI) est déterminé et accordé en fonction du besoin de savoir ou du besoin d'accéder. Cela inclut les rôles qui ont un accès hautement privilégié aux systèmes et services d'information. Les comptes privilégiés sont considérés comme étant ceux qui ont une ou plusieurs des capacités ou accès suivants :

- la capacité de modifier les principaux paramètres de configuration des systèmes;
- la capacité de modifier ou de contourner les contrôles en matière de sécurité;
- l'accès aux renseignements d'audit et de surveillance de la sécurité;
- l'accès logique et physique aux données, aux fichiers et aux comptes utilisés par d'autres utilisateurs, y compris les copies de sauvegardes et les supports;
- l'accès requis pour diagnostiquer une panne du système.

[1] Selon l'Orientation sur l'utilisation sécurisée des services commerciaux d'informatique en nuage, un fournisseur de service informatique en nuage (FSI) (https://www.canada.ca/fr/gouvernement/systeme/gouvernement-numerique/innovations-gouvernementales-numeriques/services-informatique-nuage/orientation-utilisation-securisee-services-commerciaux-informatique-nuage-amops.html#toc10) est défini comme « *une organisation non gouvernementale qui offre des services d'informatique en nuage au public ou aux clients du gouvernement dans le cadre d'une entreprise commerciale, généralement moyennant des frais avec l'intention de réaliser un profit ».*

Portée

L'entrepreneur doit mettre en œuvre des mesures de sécurité qui accordent et maintiennent le niveau requis de filtrage de sécurité pour le personnel de l'entrepreneur engagé dans la prestation de services infonuagiques et pour le personnel des sous-traitants en fonction de leurs privilèges d'accès aux actifs des systèmes d'information sur lesquels les données du gouvernement du Canada sont stockées et traitées. Lorsque l'entrepreneur est un fournisseur de SaaS ayant recours à un fournisseur d'IaaS approuvé par le GC qui se conforme déjà aux exigences de filtrage, le fournisseur de SaaS doit fournir au Canada une preuve à cet effet.

Le tableau A-1 présente les critères de filtrage des divers rôles/diverses fonctions pour les services infonuagiques commerciaux.

Tableau A-1 Guide de classification de sécurité pour les services infonuagiques commerciaux

#	Rôle/Fonction	Type prévu de données consultées	Point d'accès aux données (Canada / étranger / les deux)	Filtrage requis[2]	Détails
1.	Tout membre du personnel de l'entrepreneur ayant un accès physique aux centres de données de l'entrepreneur.	• Matériel physique. • Installations de centres de données. • Les données telles qu'elles sont stockées sur des supports de sauvegarde locaux de l'entrepreneur.	Canada	Fiabilité	Cela concerne tout le personnel de l'entrepreneur, notamment les ressources chargées de la gestion des installations qui ont physiquement accès au matériel lié aux services infonuagiques dans les centres de données de l'entrepreneur.
2.	Tout membre du personnel de l'entrepreneur ayant un accès logique aux services de l'entrepreneur.	• Toutes les données opérationnelles. • Les données telles qu'elles sont stockées dans les composantes de calcul, de stockage et de réseau de l'entrepreneur.	Les deux	Fiabilité	Cela concerne tout le personnel de l'entrepreneur qui a un accès logique aux données du GC hébergées dans les centres de données de l'entrepreneur et à tout système sensible de même qu'aux données sur les incidents de sécurité.

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

#	Rôle/Fonction	Type prévu de données consultées	Point d'accès aux données (Canada / étranger / les deux)	Filtrage requis[2]	Détails
3.	Tout membre du personnel de l'entrepreneur ayant des rôles privilégiés et un accès logique non restreint à des biens du GC au sein des services de l'entrepreneur.	• Toutes les données opérationnelles. • Les données du GC telles qu'elles sont stockées dans les composants de calcul, de stockage et de réseau de l'entrepreneur. • Données de sécurité, y compris les journaux de vérification des composantes de l'infrastructure de l'entrepreneur. • Biens, incluant notamment les données et les justificatifs du GC.	Les deux	Secret	Cela concerne le personnel de l'entrepreneur qui a des privilèges élevés assortis d'un accès logique sans restriction aux données du GC hébergées dans les centres de données de l'entrepreneur et à tout système sensible de même qu'aux données sur les incidents de sécurité.
4.	Tout membre du personnel de l'entrepreneur qui a un accès temporaire à l'information du compte maître du GC.	• Toutes les données opérationnelles. • Les données du GC telles qu'elles sont stockées dans les composants de calcul, de stockage et de réseau de l'entrepreneur. • Information du compte maître du GC.	Les deux	Fiabilité	Cela concerne tout membre du personnel de l'entrepreneur qui a accès au compte maître du GC ou aux justificatifs racines pour la configuration des comptes des services infonuagiques.
5.	Tout agent qui a accès aux renseignements de facturation du GC.	• Toutes les données opérationnelles. • Les données du GC telles qu'elles sont stockées dans les composants de calcul, de stockage et de réseau de l'entrepreneur. • Renseignements sur la facturation du GC	Les deux	Fiabilité	Cela concerne tout agent qui a accès aux renseignements du compte de facturation du GC ou aux informations qui facilitent l'accès du GC aux services infonuagiques.
6.	Entrepreneur principal*	Supports	Les deux	Fiabilité	Les informations envoyées par l'entrepreneur principal au sous-traitant doivent être chiffrées.
7.	Directeur des opérations / personnel	Nom, adresses, courriel, numéros de téléphone et centres de données	Les deux	Fiabilité	Les informations envoyées par l'entrepreneur principal au sous-traitant doivent être chiffrées.

#	Rôle/Fonction	Type prévu de données consultées	Point d'accès aux données (Canada / étranger / les deux)	Filtrage requis[2]	Détails
8.	Tâches générales	Zones publiques et d'accueil	Les deux	Sans objet	
9.	Tâches générales*	Sites sensibles (comme les zones opérationnelles où sont stockées des données).	Les deux	Fiabilité	*Les informations contenues dans ce site peuvent être de nature sensible. Les personnes ne possédant pas les attestations appropriées doivent être escortées en tout temps. Les tâches générales comprennent la prestation de services d'entretien, la présence de gardes de sécurité dans la zone opérationnelle, etc.

*L'entrepreneur doit communiquer avec le Programme de sécurité des contrats de SPAC pour s'assurer que la sous-LVERS appropriée est établie pour les sous-contractants.