

Agence de promotion économique du Canada atlantique

RÉSUMÉ DE L'ÉVALUATION DES FACTEURS RELATIFS À LA VIE PRIVÉE POUR MICROSOFT OFFICE 365

1. Aperçu et début de l'évaluation des facteurs relatifs à la vie privée

1.1 Aperçu de l'Agence de promotion économique du Canada atlantique

L'Agence de promotion économique du Canada atlantique (APECA) travaille en partenariat avec les gens du Canada atlantique afin de renforcer l'économie des collectivités et la capacité concurrentielle de la région. En collaborant avec ses partenaires du gouvernement, du secteur privé, des universités et d'autres secteurs non gouvernementaux, l'APECA cherche à promouvoir les débouchés économiques et l'innovation afin de répondre aux besoins des entreprises, des organisations, des particuliers et des collectivités. Elle remplit ainsi son mandat, soit de « favoriser la croissance des revenus et la création d'emplois au Canada atlantique ».

Avec ses nombreux partenaires participant au développement économique, l'APECA s'efforce de consolider l'économie du Canada atlantique comme suit :

- Développement des entreprises – contribuer à améliorer le climat commercial et contribuer au démarrage d'entreprises ainsi qu'à leur modernisation et à leur expansion.
- Développement des collectivités – collaborer avec les collectivités pour favoriser la croissance économique, améliorer les infrastructures et créer des possibilités dans l'économie locale.
- Politique, défense des intérêts et coordination – être un champion pour le Canada atlantique en défendant les intérêts régionaux au niveau national dans des secteurs tels que l'élaboration de politiques ainsi que la recherche et l'analyse, et dans divers travaux avec d'autres ministères pour garantir la coordination des politiques et des programmes.

L'APECA est assujettie au régime de responsabilisation établi dans la partie II de la Loi sur la gestion des finances publiques (LGFP) et est mentionnée dans les annexes IV et VI de la LGFP.

1.2 Harmonisation avec les politiques du gouvernement du Canada

La *Directive sur l'évaluation des facteurs relatifs à la vie privée* (EFVP) du Conseil du Trésor oriente les institutions gouvernementales sur la façon d'évaluer ces facteurs liés aux programmes ou aux activités nouveaux ou substantiellement modifiés comprenant la création, la collecte et le traitement de renseignements personnels. Elle garantit également que les répercussions sur la vie privée sont bien cernées, évaluées et réglées avant l'établissement ou la modification importante d'un programme ou d'une activité impliquant des renseignements personnels.

Hiérarchie des politiques du gouvernement du Canada

- *Loi sur la protection des renseignements personnels*
 - Politique sur la protection de la vie privée
 - Directive sur l'évaluation des facteurs relatifs à la vie privée
 - Directive sur les pratiques relatives à la protection de la vie privée
 - Directive sur le numéro d'assurance sociale

1.3 Description de l'initiative

M365 est la nouvelle plateforme numérique du gouvernement du Canada (GC) visant à améliorer la façon dont les employés fédéraux communiquent et collaborent avec leurs collègues et servent les Canadiens.

Microsoft Canada Inc. a commandé des EFVP indépendantes de sa plateforme infonuagique Microsoft Office 365 ainsi que son infrastructure-service et plateforme-service Azure. Ces documents se trouvent sur la page [Ressources sur la conformité pour le Canada](#) de Microsoft.

L'APECA est l'un des cinq ministères choisis par Service partagés Canada (SPC) comme orienteurs pour déployer Microsoft 365 (M365) auprès de tous les employés. Cette suite logicielle comprend entre autres des versions actualisées et multiplateformes d'Outlook, Word, PowerPoint, Excel et Teams. SPC a recommandé que chaque ministère prévoyant migrer vers M365 effectue sa propre EFVP afin d'établir les risques et les mesures d'atténuation en tenant compte de son infrastructure, de ses éléments de données, de ses charges de travail et de sa configuration de locataires. L'EFVP du PCCN d'entreprise de SPC servira de base à cette tâche.

M365 est une puissante suite d'applications permettant à l'APECA de mieux collaborer, d'accélérer ses communications dans toute l'organisation et d'atteindre ses objectifs de croissance et opérationnels. Elle comprend de nombreuses fonctions et capacités qui faciliteront la transition de l'Agence vers une organisation numérique capable de fonctionner pratiquement n'importe où, n'importe quand. Cette initiative insiste sur la transition de la suite actuelle de produits Microsoft Office (Outlook, PowerPoint, Word et Excel) de l'APECA et de son lecteur réseau personnel, passant d'un stockage sur site vers un stockage infonuagique. Les solutions que l'APECA met à profit sont Office 365 et One Drive for Business, deux produits Microsoft (MS). Cette solution optimisera un modèle de logiciel service (SaaS). Les renseignements de l'APECA seront stockés et traités dans des centres de données situés au Canada.

MS Teams

- MS Teams constitue le cœur de vos interactions dans M365 en offrant des fonctions de clavardage, d'audioconférence et de vidéoconférence.
- Un espace de travail virtuel Teams signifie qu'il existe toujours une salle de conférence disponible où les employés peuvent se réunir, peu importe où ils se trouvent.
- La fonction de clavardage dans Teams permet aux employés d'interagir rapidement avec leurs collègues lorsqu'un courriel n'est pas requis.

Exchange Online

- Les outils infonuagiques de M365 synchronisent les courriels, calendriers, tâches et coordonnées dans Exchange Online sur tous les appareils en temps réel afin qu'ils soient à jour, peu importe l'appareil utilisé. La planification est facile et sans souci.
- Exchange Online aide les employés à collaborer à des documents critiques et leur procure une boîte de réception organisée qui priorise les messages importants et s'adapte à leur style de travail afin qu'ils puissent en faire plus, plus rapidement.

OneDrive

- OneDrive est la plateforme personnelle de stockage infonuagique de M365 donnant un accès rapide et facile aux fichiers à partir de n'importe quel appareil mobile ou appareil informatique du GC.
- OneDrive rend obsolètes les limites de taille des pièces jointes de courriel. Par Teams ou Outlook, les employés peuvent partager un lien vers leur document dans OneDrive qui permet aux collègues de le lire ou d'y travailler pendant qu'il demeure sauvegardé dans leur lecteur personnel.

Infonuagique/sécurité/mobilité

- Les outils infonuagiques de M365 permettent aux employés de passer facilement des appareils mobiles aux appareils informatiques du GC tout en continuant d’avoir accès à leurs documents et messages, même lorsqu’ils sont en déplacement.
- Ces outils offrent un accès sécurisé de calibre mondial à partir de n’importe quel appareil mobile ou informatique du GC; les employés peuvent ainsi travailler sur des documents de niveau Protégé B, peu importe où ils sont.

1.4 Objectif de l’évaluation

L’objectif de cette EFVP consiste à déterminer comment l’adoption de Microsoft Office 365 par l’APECA pourrait avoir un impact sur la vie privée d’une personne. L’EFVP est un moyen pour l’Agence d’affirmer son engagement à protéger la vie privée des personnes alors qu’elle fait la promotion de la transparence et de la responsabilisation, et elle contribue à maintenir la confiance dans la façon dont l’Agence gère les renseignements personnels.

1.5 Autorisations législatives

Loi sur l’Agence de promotion économique du Canada atlantique

Conformément à cette loi, l’objectif de l’Agence consiste à soutenir et à promouvoir les occasions de développement économique au Canada atlantique par des mesures – élaboration et mise en œuvre d’orientations, de programmes et d’opérations – particulières, notamment en faveur des petites et moyennes entreprises (PME), et par la défense des intérêts du Canada atlantique lors de la prise de mesures de ce genre dans le cadre de la politique économique nationale. Son but est d’accroître les occasions de développement économique au Canada atlantique et, plus particulièrement, de favoriser la croissance des revenus et la création d’emplois dans la région.

Loi sur la gestion des finances publiques

L’Agence est assujettie au régime de responsabilisation établi dans la LGFP. L’APECA est mentionnée dans les annexes I.1 et IV de la LGFP.

1.6 Éléments des renseignements personnels

Les fichiers de renseignements personnels (FRP) sont des descriptions de renseignements personnels relevant de la compétence d’une institution gouvernementale, qui sont organisées et consultables par nom de personne ou par numéro, symbole ou autre élément identifiant cette personne. Les renseignements personnels décrits dans un FRP ont été utilisés, sont utilisés ou sont accessibles à des fins administratives. Le FRP décrit comment les renseignements personnels sont recueillis, utilisés, divulgués, conservés ou détruits dans le cadre de l’administration d’un programme ou d’une activité d’une institution gouvernementale. Les FRP ordinaires décrivent les renseignements sur les membres du public ainsi que les employés fédéraux actuels ou anciens contenus dans des documents créés, recueillis et tenus à jour par la plupart des institutions gouvernementales à l’appui des services internes courants. Cela comprend les renseignements personnels liés à la gestion des ressources humaines, aux déplacements, aux communications organisationnelles et à d’autres services administratifs. Les FRP ordinaires sont créés par le Secrétariat du Conseil du Trésor du Canada. Une description des FRP ordinaires de l’APECA qui suivent se trouve dans le document [Info Source du Secrétariat du Conseil du Trésor](#).

Titres des FRP ordinaires de l'APECA	N° du fichier
Accès à l'information et protection des renseignements personnels	PSU 901
Comptes créditeurs	PSU 931
Comptes débiteurs	PSU 932
Cartes d'achat	PSU 940
Demandes d'emploi	PSU 911
Présence et congés	PSE 903
Planification de la continuité des activités	PSU 903
<i>Loi canadienne sur les droits de la personne – plaintes</i>	PSU 933
Mesures disciplinaires	PSE 911
Divulgence d'actes fautifs commis en milieu de travail	PSU 906
Divulgence aux organismes d'enquête	PSU 913
Registres de surveillance des réseaux électroniques	PSU 905
Aide aux employés	PSE 916
Programme de gestion du rendement des employés	PSE 912
Dossier personnel d'un employé	PSE 901
Équité en matière d'emploi et diversité	PSE 918
Correspondance de la direction	PSU 902
Évaluation	PSU 942
Gestion des talents des cadres supérieurs	PSU 934
Nominations par le gouverneur en conseil	PSU 918
Griefs	PSE 910
Harcèlement	PSE 919
Accueil	PSU 908
Planification des ressources humaines	PSE 935
Cartes d'identité et laissez-passer	PSU 917
Vérification interne	PSU 941
Communications internes	PSU 915
Services de bibliothèque	PSU 936
Exigences de la <i>Loi sur le lobbying</i>	PSU 937
Membres de conseils d'administration, de comités et de conseils	PSU 919
Santé et sécurité au travail	PSE 907
Langues officielles	PSE 906
Activités de sensibilisation	PSU 938
Rémunération et avantages sociaux	PSE 904

Filtrage de sécurité du personnel	PSU 917
Contrats de services professionnels	PSU 912
Communications publiques	PSU 914
Gestion des biens immobiliers	PSU 948
Programme de reconnaissance	PSE 920
Réinstallation	PSU 910
Incidents de sécurité et atteintes à la vie privée	PSU 939
Surveillance vidéo, registres de contrôle d'accès des visiteurs et laissez-passer	PSU 907
Dotation	PSE 902
Formation et perfectionnement	PSE 905
Voyages	PSU 909
Codes de valeurs et d'éthique du secteur public et codes de conduite organisationnels	PSE 915
Accidents d'automobile, de bateau, d'embarcation et d'avion	PSE 908

Titres des FRP propres à l'APECA	N° du fichier	No d'enregistrement SCT
• Subventions et contributions	APECA PPU 005	007070
Description : Ce fichier décrit les renseignements recueillis à l'appui de demandes de subventions et de contributions qui proviennent de personnes, du gouvernement fédéral ou de gouvernements provinciaux, d'organismes, de sociétés et de municipalités, ainsi que des documents nécessaires pour confirmer que le bénéficiaire a respecté les exigences de l'entente de contribution. Les renseignements personnels peuvent comprendre le nom, les coordonnées, les préférences linguistiques, des renseignements biographiques, des références professionnelles, la signature, des renseignements financiers, la date de naissance, le numéro d'assurance sociale (NAS) et des photographies. Catégorie de personnes : Personnes, propriétaires uniques, partenaires d'affaires, fonctionnaires et employés d'un organisme, d'une société ou d'une municipalité. But : Ces renseignements personnels sont recueillis pour évaluer et traiter les demandes de financement en vertu de la <i>Loi sur l'Agence de promotion économique du Canada atlantique</i> (APECA) et de la LGFP. Le NAS est recueilli conformément à la <i>Loi de l'impôt sur le revenu</i>. Usages compatibles : Le nom des demandeurs retenus ainsi que certains autres renseignements pertinents figurent dans les documents publics et sont publiés sur le site Web de l'Agence, conformément aux pratiques de divulgation proactive du gouvernement du Canada. Après avoir obtenu le consentement des parties concernées, l'APECA peut publier des renseignements personnels dans ses histoires de réussite. L'information peut être utilisée aux fins de vérification interne, d'évaluation ou de préparation de rapports.		

Titres des FRP propres à l'APECA	N° du fichier	No d'enregistrement SCT
• Pairs examinateurs	APECA PPU 111	20090345
Description : Ce fichier contient des renseignements recueillis par des pairs examinateurs à l'appui des examens scientifiques des propositions de projet d'un promoteur en vue de l'obtention d'un financement dans le cadre du FIA. Ces renseignements personnels peuvent comprendre le nom, les coordonnées, des renseignements financiers ou contractuels, les préférences linguistiques, des renseignements biographiques, les études, les antécédents professionnels, des références professionnelles, la signature et le NAS. Catégorie de personnes : Les personnes travaillant dans des domaines scientifiques et novateurs particuliers qui effectuent un examen par les pairs de promoteurs de projets scientifiques. But : Les renseignements personnels sont recueillis pour évaluer les compétences des pairs qui examinent les propositions de projet présentées en vue de l'obtention d'un financement dans le cadre du FIA, pour rémunérer leurs services, le cas échéant, et pour avoir un répertoire de pairs examinateurs. Le NAS est utilisé aux fins de l'impôt sur le revenu en vertu de la <i>Loi de l'impôt sur le revenu</i>. Usages compatibles : Une liste des pairs examinateurs est tenue à jour aux fins de rappel. Les renseignements peuvent être communiqués à l'Agence du revenu du Canada (ARC); voir la Banque de données des déclarations de renseignements (Infodéc) ARC PPU 150. Les renseignements peuvent également être utilisés aux fins d'évaluation ou de présentation de rapports à l'intention de la haute direction.		

1.7 Analyse de la conformité en matière de protection des renseignements personnels (dix principes de protection des renseignements personnels)

Bien qu'il n'y ait aucun changement à ces dix principes, l'emplacement du stockage et les moyens d'y accéder ont changé avec le passage à l'infonuagique. Il importe de noter que Microsoft ne recueille pas les renseignements personnels autres que les données des employés pour l'inscription des utilisateurs – renseignements que l'APECA leur fournira.

Principe 1 : responsabilisation

L'APECA est responsable de tous les renseignements personnels recueillis et utilisés en vertu de la *Loi sur l'APECA*. Les instruments de politique internes suivants ont été élaborés afin d'informer tous les employés de leurs responsabilités.

- **Les pratiques efficaces de protection de la vie privée de l'APECA** doivent être suivies par tous les employés participant aux activités liées à la création, à la collecte, à la conservation, à l'exactitude, à l'utilisation, à la divulgation ou à la destruction de renseignements personnels relevant de la compétence de l'APECA, notamment les renseignements personnels des employés de l'Agence.
- **Le protocole de protection de la vie privée de l'APECA** permet de s'assurer que la collecte, l'utilisation ou la divulgation de renseignements personnels à des *fins non administratives* sont menées conformément à la *Loi sur la protection des renseignements personnels*, au règlement sur la protection des renseignements personnels et aux exigences connexes de la politique de protection des renseignements personnels du Secrétariat du Conseil du Trésor.

- **Les procédures de l'APECA à suivre en cas d'atteinte à la vie privée** décrivent les rôles et responsabilités des employés de l'Agence quant à la gestion des atteintes à la vie privée ainsi qu'aux procédures et communications internes (notamment le moment) pour donner un avis au Commissariat à la protection de la vie privée, au Secrétariat du Conseil du Trésor et aux autres parties touchées par ces atteintes. Elles visent aussi les exigences générales des articles 4 à 6 de la [Loi sur la protection des renseignements personnels](#) concernant la collecte, la conservation, l'utilisation, la divulgation et la destruction des renseignements personnels.
- Le **Manuel de gestion de l'information pour les employés de l'APECA** énumère les rôles et responsabilités des employés en matière de collecte, d'utilisation et de gestion des renseignements.
- Les représentants de l'Agence doivent suivre une **séance d'information standard sur la sécurité du gouvernement du Canada**. Pendant cette séance, les personnes sont informées de leurs responsabilités en vertu de la [Politique sur la sécurité du gouvernement](#) et des permissions d'accès liées à leur niveau de filtrage. La séance offre l'occasion aux gens de poser des questions et de mieux comprendre ces responsabilités. Elle officialise également l'attribution d'une cote de fiabilité ou de sécurité, ainsi que l'acceptation par la personne concernée des responsabilités en matière de sécurité et son engagement à s'y conformer. Les séances d'information sur la sécurité sont menées à diverses périodes : avant qu'une personne n'entre en fonction, au besoin selon le cycle de mise à jour et lorsqu'un changement survient dans le niveau de filtrage.

Pour la présente initiative, le dirigeant principal de l'information et la directrice de l'Accès à l'information et de la protection des renseignements personnels doivent veiller à ce que l'organisation respecte les principes suivants. Les employés sont tenus de respecter les politiques et procédures suivantes afin de s'assurer que l'organisation demeure conforme aux principes ci-après.

Principe 2 : objectif

L'Agence ne recueille que les renseignements personnels requis pour s'acquitter de son mandat, comme défini dans la *Loi sur l'APECA*, et dont la collecte est autorisée par la loi.

Principe 3 : consentement

L'Agence utilise des énoncés de confidentialité et Info Source afin d'informer les personnes concernées des renseignements qu'elle recueille, des raisons de cette collecte, des droits des personnes relativement à l'accès à ces renseignements et à leur correction, ainsi que des destinataires susceptibles de recevoir ces renseignements.

L'Agence informera ses employés par courriel concernant M365 et le passage aux services infonuagiques. À l'externe, l'Agence publiera un avis sur son site Web comme annonçant qu'elle utilise les services infonuagiques pour stocker certains de ses renseignements.

Principe 4 : limiter la collecte

L'autorisation précise de l'APECA pour la collecte de renseignements personnels relève de la *Loi sur l'APECA*. Les détails de la collecte sont inclus dans les FRP ordinaires et propres à l'APECA, qui sont énumérés ci-dessous (après les dix principes de protection des renseignements personnels).

Principe 5 : limiter l'utilisation, la divulgation et la conservation

La **politique et directive sur l'accès aux réseaux** de l'APECA permet de s'assurer que les utilisateurs autorisés reconnaîtront l'utilisation appropriée du réseau électronique de l'APECA.

- **Utilisation** : L'accès à l'information est contrôlé par des autorisations de sécurité et le besoin de savoir, et l'utilisation est fondée sur les tâches d'un employé ainsi que les politiques, protocoles et procédures opérationnelles normalisées mis en place.
- **Divulgation** : L'APECA ne divulguera pas de renseignements personnels sans le consentement de la personne à moins que l'Agence ne soit légalement autorisée à le faire conformément à la *Loi sur la protection des renseignements personnels*.
- **Conservation** : Les calendriers de conservation et de destruction de l'APECA s'appliquent principalement à ses documents administratifs courants. Les règles de conservation de ces documents sont conformes aux outils génériques d'évaluation produits par Bibliothèque et Archives Canada. Les renseignements personnels détenus par l'Agence seront conservés pendant au moins deux ans après l'achèvement d'une mesure administrative.

Principe 6 : exactitude

Les secteurs opérationnels de l'APECA qui traitent les renseignements personnels doivent s'assurer que les renseignements sont exacts, complets et à jour. En plus des instruments de politique élaborés par le Secrétariat du Conseil du Trésor, l'Agence a produit des documents qui aident ses employés à utiliser, à repérer et à traiter les renseignements personnels, soit :

- Manuel de gestion de l'information
- Protocole de protection de la vie privée
- Manuel d'évaluation des facteurs relatifs à la vie privée
- Pratiques efficaces de protection de la vie privée de l'APECA

Principe 7 : mesures de protection des renseignements personnels

L'APECA prend les mesures nécessaires pour protéger les renseignements personnels relevant de sa compétence. L'Agence possède un cadre de politiques, directives et procédures pour protéger ces renseignements contre la perte, le vol, l'accès non autorisé ou la divulgation, et propose une combinaison de formations obligatoires et facultatives afin de sensibiliser ses employés à leurs rôles et responsabilités liés à la protection des renseignements personnels. L'Agence emploie des mesures physiques, opérationnelles et technologiques pour protéger ces renseignements.

- **Mesures de protection physiques :**

La Directive sur la gestion de la sécurité exige que des mesures de protection soient mises en œuvre pour garantir la confidentialité des renseignements pendant qu'ils sont stockés, traités ou transmis, l'intégrité des renseignements et des processus, la disponibilité des renseignements et des systèmes et services connexes, ainsi que la protection du personnel et des biens.

- Tous les employés, entrepreneurs et bénévoles font l'objet d'une vérification de leur fiabilité, au minimum.
- Les employés, entrepreneurs et visiteurs doivent porter leur carte d'identité ou laissez-passer en tout temps.
- Les visiteurs doivent être accompagnés en tout temps à l'entrée et à la sortie des zones opérationnelles et de sécurité de l'APECA.
- Les renseignements d'ordre physique sont stockés dans une armoire verrouillée adaptée à leur niveau de sécurité.

- Seuls les employés ayant besoin de savoir et possédant le filtrage de sécurité approprié peuvent accéder aux renseignements requis pour accomplir leur travail.
 - La destruction des renseignements papier sensibles est effectuée par des déchiqueteurs du GC approuvés ou des entrepreneurs ayant l'équipement et le filtrage de sécurité répondant aux lignes directrices de la GRC.
- **Mesures de protection technologiques :**
 - La politique sur la sécurité des technologies de l'information (TI) de l'APECA a été conçue pour s'assurer que l'Agence gère efficacement ses activités liées à la sécurité des TI et contribue à une gestion pangouvernementale efficace de la sécurité.
 - La directive ministérielle sur la sécurité des TI établit les objectifs de contrôle minimaux de la sécurité des TI que l'Agence doit atteindre afin de s'assurer que son mandat, ses activités, ses priorités et ses exigences de sécurité sont respectés.
 - L'Agence a aussi élaboré le **Manuel de gestion de l'information pour les employés de l'APECA**, qui présente les éléments fondamentaux que les employés doivent connaître pour s'acquitter de leurs responsabilités en matière de gestion de l'information.
 - Microsoft utilise des mesures de contrôle correspondant à la publication ITSG-33 du Centre canadien pour la cybersécurité. Ce document a été élaboré afin d'aider les ministères à s'assurer que la sécurité est prise en compte dès le début. En suivant les principes énoncés dans ce document, l'APECA permet de garantir non seulement la prévisibilité et le rapport coût-efficacité, mais aussi qu'aucune surprise ne l'empêche d'obtenir une autorisation d'exploitation et de maintenir cette autorisation.
 - Une surveillance continue des mesures de protection aidera l'APECA à établir comment ses lignes directrices et politiques internes, entre autres, peuvent devoir être modifiées pour mieux s'adapter à l'environnement en évolution.

Principe 8 : ouverture

L'APECA divulgue proactivement des renseignements afin que les Canadiens et le Parlement soient mieux positionnés pour rendre l'Agence imputable. Diverses publications de l'Agence accessibles au public se trouvent sur le [site Web de l'APECA](#).

Principe 9 : accès aux renseignements personnels

La Loi sur la protection des renseignements personnels accorde à chaque personne le droit de recevoir l'accès aux renseignements personnels portant sur cette personne et contenus dans un FRP, ainsi qu'à tout autre renseignement personnel sur cette personne relevant d'une institution gouvernementale. Lorsque les renseignements personnels servent à des fins administratives, la personne est autorisée à demander la correction de toute erreur ou omission.

La collecte de renseignements personnels détenus par l'APECA tombe dans la catégorie des FRP ordinaires ou propres à l'APECA inscrits auprès du Secrétariat du Conseil du Trésor (SCT). La description des FRP ordinaires inscrits par l'APECA est accessible dans [Info Source du SCT](#), sur sa page Web [Accès à l'information et protection des renseignements personnels](#). L'Agence a inscrit deux FRP propres à l'APECA et liés à ses programmes; une description est accessible dans son [Info Source](#). La publication donne également une description des programmes et des fonds de renseignements de l'APECA.

Les personnes peuvent demander l'accès ou une correction à leurs renseignements personnels en communiquant avec la coordonnatrice de l'accès à l'information et de la protection des renseignements personnels de l'APECA par téléphone au 506-871-2806 ou par courriel à atip-aiprp@acoa-apeca.gc.ca.

Principe 10 : contestation de la conformité

Une personne peut déposer une contestation touchant la conformité de l'APECA à ces principes. Toute plainte peut être adressée à la coordonnatrice de l'accès à l'information et de la protection des renseignements personnels de l'APECA par téléphone au 506-871-2806 ou par courriel à atip-aiprp@acoa-apeca.gc.ca.

De plus, en vertu de la Loi sur la protection des renseignements personnels, les personnes peuvent déposer une plainte officielle auprès du Commissariat à la protection de la vie privée du Canada si elles estiment que leurs renseignements personnels ont été traités de façon inappropriée. Vous trouverez de plus amples renseignements sur la page Signaler des préoccupations du Commissariat.

1.8 Tableau des flux des renseignements personnels

À L'INTÉRIEUR DU NUAGE MICROSOFT			À L'EXTÉRIEUR DU NUAGE MICROSOFT			
EMPLOYÉS DE L'APECA - AU TRAVAIL - À LA MAISON - EN DÉPLACEMENT	CHIFFRÉS 	CHIFFRÉS (Office 365)	NON CHIFFRÉS 	SERVEUR DE COURRIEL EXTERNE	NON CHIFFRÉS 	UTILISATEUR DE COURRIEL EXTERNE

À l'intérieur du nuage :

- courriels (avec ou sans pièce jointe) destinés à des employés de l'APECA ou provenant d'eux;
- renseignements contenus dans One Drive;
- sauvegarde de données.

À l'extérieur du nuage :

- courriels (avec ou sans pièce jointe) envoyés par des employés de l'APECA à des comptes de courriel autres que l'APECA (les employés peuvent toujours chiffrer les renseignements grâce à une ICP au besoin);
- courriels (avec ou sans pièce jointe) envoyés à des employés de l'APECA par des parties externes.

2. Identification et catégorisation des zones à risque

2.1 Type d'activité	Niveau de risque
Programme ou activité ne comprenant PAS de décision sur une personne identifiable	☐ 1
Administration de programmes, activités et services	☒ 2
Enquêtes de conformité et réglementaires, et application	☐ 3
2.2 Type de renseignements personnels et contexte	Niveau de risque
Seulement les renseignements personnels sans sensibilité contextuelle, recueillis directement auprès de la personne ou fournis avec son consentement aux fins de divulgation en vertu d'un programme autorisé.	☐ 1
Les renseignements personnels, sans sensibilité contextuelle après le moment de la collecte, fournis par la personne avec son consentement en vue d'utiliser également les renseignements personnels détenus par une autre source.	☐ 2
Le numéro d'assurance sociale, les renseignements médicaux, financiers ou autres renseignements personnels sensibles, ou le contexte sensible entourant ces renseignements; les renseignements personnels de mineurs ou de personnes légalement incompetentes ou impliquant un représentant qui agit au nom de la personne.	☒ 3
Les renseignements personnels sensibles, notamment les profils détaillés, allégations ou soupçons et échantillons personnels, ou le contexte particulièrement sensible entourant ces renseignements.	☐ 4
2.3 Partenaires du programme ou de l'activité et participation du secteur privé	Niveau de risque
- Au sein de l'institution (parmi un ou plusieurs programmes dans la même institution)	☐ 1
- Autres institutions gouvernementales	☐ 2
- Autres institutions ou combinaison d'administrations fédérale, provinciales ou territoriales et municipales	☐ 3
- Organisations du secteur privé, organisations internationales ou gouvernements étrangers	☒ 4
Détails : Les renseignements de l'APECA seront stockés et traités dans des centres de données Microsoft du Canada.	
2.4 Durée du programme ou de l'activité	Niveau de risque
- Programme ou activité ponctuel	☐ 1
- Programme ou activité à court terme	☐ 2
- Programme ou activité à long terme	☒ 3
2.5 Population du programme	Niveau de risque
- L'utilisation par le programme des renseignements personnels à des fins administratives internes touche certains employés.	☐ 1
- L'utilisation par le programme des renseignements personnels à des fins administratives internes touche tous les employés.	☐ 2
- L'utilisation par le programme des renseignements personnels à des fins administratives externes touche certains employés.	☐ 3

- L'utilisation par le programme des renseignements personnels à des fins administratives externes touche tous les employés.	☒ 4	
2.6 Technologie et protection de la vie privée	Risque d'atteinte à la vie privée	
Le programme ou l'activité nouveau ou modifié comprend-il la mise en œuvre d'un <u>nouveau système électronique</u> , logiciel ou programme d'application, notamment un logiciel de collaboration (ou collecticiel) qui appuiera le programme ou l'activité en matière de création, de collecte ou de traitement de renseignements personnels?	☒ OUI ☐ NON	
Le programme ou l'activité nouveau ou modifié nécessite-t-il des modifications aux <u>services ou systèmes informatiques existants</u> ?	☒ OUI ☐ NON	
Le programme ou l'activité nouveau ou modifié comprend la mise en œuvre d'une ou plusieurs des technologies suivantes :		
Méthodes d'identification améliorées Dans l'affirmative, donnez des détails :	☒ OUI ☐ NON	
Utilisation de la surveillance Dans l'affirmative, donnez des détails :	☒ OUI ☐ NON	
Utilisation de techniques automatisées d'analyse et de mise en correspondance des renseignements personnels et de découverte des connaissances : (dans l'affirmative, donnez des détails).	☒ OUI ☐ NON	
Détails : • Authentification à deux facteurs • Surveillance de l'adresse IP, géoblocage, etc. • Divulgaration de renseignements protégés et protection accrue (p. ex., NAS)		
2.7 Transmission des renseignements personnels	Niveau de risque	
- Les renseignements personnels sont utilisés dans un système fermé (c.-à-d. aucune connexion à Internet, à l'intranet ou à un autre système, et circulation de documents papier contrôlée).	☐ 1	
- Les renseignements personnels sont utilisés dans un système connecté à au moins un autre système.	☐ 2	
- Les renseignements personnels sont transférés à un appareil portable (p. ex., clé USB, disquette, ordinateur portable), transférés à un support différent ou imprimés.	☐ 3	
- Les renseignements personnels sont transmis au moyen de technologies sans fil.	☒ 4	
Détails : Les applications de M365 sont offertes au moyen d'une plateforme Internet en ligne, et les données sont stockées dans un environnement infonuagique situé au Canada et hébergé par Microsoft. Les employés accèdent seulement aux renseignements requis pour s'acquitter de leurs responsabilités au moyen du Wi-Fi ou du RPV organisationnel sécurisé, grâce à l'équipement fourni par l'APECA.		
2.8 Impact d'une atteinte à la vie privée sur les personnes	Oui	Non
Risque d'impact sur la personne ou l'employé en cas d'atteinte à la vie privée.	☒	☐

Détails : En cas d'atteinte à la vie privée impliquant des renseignements personnels courants non sensibles, l'impact pour les personnes touchées peut être considéré comme minime. Cependant, cet impact peut s'accroître selon la sensibilité des renseignements personnels, ce qui peut causer de l'embarras pour la personne. L'Agence a élaboré des procédures pour résoudre les atteintes à la vie privée.

2.9 Impact d'une atteinte à la vie privée sur une institution	Oui	Non
Risque d'impact sur l'institution en cas d'atteinte à la vie privée.	☒	☐
Détails : En cas d'atteinte à la vie privée impliquant des renseignements personnels courants non sensibles, l'impact pour l'institution peut être considéré comme minime. Cependant, cet impact peut s'accroître selon la sensibilité des renseignements personnels, ce qui peut causer de l'embarras pour l'institution. L'Agence a élaboré des procédures pour résoudre les atteintes à la vie privée.		
2.10 Impact du risque pour l'Agence	Niveau de risque	
Préjudice pour la direction Les processus doivent être révisés, les outils doivent être changés et il faut changer de fournisseur/partenaire.	☐ 1	
Préjudice organisationnel Changements à la structure organisationnelle, à la structure décisionnelle de l'organisation, à la distribution des responsabilités ainsi qu'à l'architecture d'activités de programme, départ d'employés, réattribution des RH.	☐ 2	
Préjudice financier Des poursuites et des sommes additionnelles ont nécessité une réattribution des ressources financières.	☐ 3	
Atteinte à la réputation, embarras, perte de crédibilité Confiance décroissante du public, élus sous les feux de la rampe, résultats stratégiques compromis d'une institution ou priorité gouvernementale compromise.	☒ 4	
2.11 Impact du risque pour les personnes ou employés	Niveau de risque	
Inconvénients	☐ 1	
Atteinte à la réputation, embarras	☐ 2	
Préjudice financier	☒ 3	
Préjudice physique	☐ 4	

2.12 Exemple de renseignements personnels et de leur parcours à l'extérieur de l'APECA

Description/but	Type
Courriel reçu d'un client qui demande un service et fournit de la rétroaction.	Collecte
Courriel de réponse envoyé au client pour demander des renseignements supplémentaires, proposer une résolution ou accuser réception.	Divulgarion
Demande de service transférée au fournisseur de services engagé par l'APECA.	Divulgarion et utilisation
Courriel reçu du fournisseur de services engagé par l'APECA.	Collecte
Courriel envoyé à une partie externe selon des exigences prévues par la loi ou liées aux processus.	Divulgarion et utilisation

2.13 Avis de collecte

L'APECA dispose déjà d'outils pour conseiller les particuliers qui donnent des renseignements personnels sur le but, l'autorisation législative, l'utilisation, la divulgation, les conséquences, le droit d'accès et la correction, la référence du FRP et le droit de déposer une plainte concernant leur collecte.

L'Agence inclura un énoncé de confidentialité pour le passage vers des services infonuagiques. Cet énoncé sera accessible aux employés internes et au public externe. Toutes les questions initiales liées à cet énoncé seront acheminées au bureau de l'accès à l'information et de la protection des renseignements personnels.

2.14 Sécurité des renseignements personnels

Ce FRP porte sur un système d'information fondé sur l'infonuagique. Services partagés Canada est le dépositaire de la majeure partie de l'infrastructure informatique gouvernementale. SPC collabore avec les ministères et agences afin d'aider à prévenir les cybermenaces et les intrusions injustifiées en protégeant et en sécurisant l'intégrité des réseaux et des renseignements gouvernementaux.

L'ensemble des éléments liés à la sécurité informatique est assuré par une évaluation distincte appelée processus d'évaluation et d'autorisation de sécurité (EAS). SPC appuie l'APECA par son service d'EAS afin d'assurer la confidentialité, l'intégrité et la disponibilité de ses systèmes et données.

L'Agence possède ses propres politiques, directives et lignes directrices en matière de sécurité en plus de la politique sur la sécurité du gouvernement du SCT.

2.15 Mesures de sécurité physiques relatives à l'initiative

Sécurité de l'installation Microsoft

- Sécurité du périmètre : les centres de données ont du personnel de sécurité sur place en tout temps. Les bâtiments sont sans caractère particulier et n'affichent pas que des services d'hébergement des centres de données de Microsoft y sont offerts.
- Surveillance : les centres sont surveillés par des détecteurs de mouvement, par surveillance vidéo et des alarmes d'intrusion.
- Contrôles d'accès physique : l'authentification multifacteur est utilisée, notamment la lecture biométrique, les systèmes d'identification, les insignes et les cartes à puce afin d'accorder l'accès aux centres.
- Salles informatiques : elles sont équipées d'un système de contrôle d'accès à deux facteurs constitué de lecteurs biométriques et de lecteurs de cartes.
- Isolation : le réseau interne de centres de données est isolé du réseau externe.
- Alimentation : des sources d'alimentation ininterrompues et des générateurs au diesel sont installés en cas de panne de courant.
- Mesures additionnelles : séparation des rôles, démagnétisation et destruction physique des disques durs défectueux et destruction physique des disques durs mis hors service.

2.16 Mesures de sécurité technologiques relatives à l'initiative

- Le fournisseur de services infonuagiques utilise l'isolation de données (dans un environnement multilocataire).
- Il utilise des systèmes divisés en partitions logiques à l'aide d'un réseau local virtuel.

- Il utilise les fonctions de pare-feu, de traduction d'adresses de réseau et de filtrage IP.
- Il utilise la détection et la prévention des intrusions réseau.
- Il effectue l'installation des mises à jour de sécurité prévues pour le système d'exploitation.
- Il offre une authentification multifacteur pour l'accès aux services.
- Il mène une analyse des vulnérabilités sur les serveurs hébergeant des données de locataire et des appareils de périmètre.

2.17 Atténuer les contrôles d'accès

Microsoft limitera ou restreindra l'accès non autorisé aux renseignements personnels, notamment les changements comme les ajouts ou suppressions, ce qui garantit :

- la séparation des tâches afin de rendre illisible l'emplacement de certaines données relatives aux clients pour le personnel ayant un accès physique;
- que les politiques et procédures appliquent les contrôles d'accès selon le principe du privilège minimal pour les systèmes opérationnels et les données d'abonné/locataire;
- que le personnel signe des ententes de confidentialité et de non-divulgateur;
- l'utilisation d'Azure Active Directory pour l'attribution des comptes, laquelle est fondée sur le modèle de locataires et sépare les multilocataires en contenants logiques discrets.

Comment les personnes accédant aux renseignements personnels sans autorisation seront identifiées :

- Microsoft (fournisseur de services infonuagiques) et l'APECA (locataire) disposent de pratiques de gestion et d'intervention en cas d'incident bien documentées.
- Office 365 peut être configuré pour respecter les politiques de vérification. Cela permet à l'APECA de consigner des événements précis, notamment visualiser, réviser et supprimer du contenu (p. ex., courriels, documents, listes de tâches, listes de problèmes, groupes de discussion et calendriers).

Complément d'information

L'APECA ne donne pas accès aux données à caractère personnel aux fins de recherche ou de statistiques.

Aucun des FRP actuels de l'APECA n'est touché par cette initiative. Les renseignements personnels continueront d'être créés ou recueillis comme décrit dans les FRP propres à l'Agence et ordinaires.

Intervenants

Nom	Rôle	Coordonnées
Louise Doucet	Directrice-coordonnatrice Accès à l'information et protection des renseignements personnels	louise.doucet@acoa-apec.gc.ca
Marc Gagnon	Directeur général Direction du dirigeant principal de l'information	marc.gagnon@acoa-apec.gc.ca