Canadian Association of Professional Immigration Consultants

L'Association Canadienne des Conseillers Professionnels en Immigration

Politique de gouvernance des TI et d'atténuation des risques

Approuvée initialement le 3 décembre 2024
Modifiée et approuvée en avril 2026

Classification	Interne
Autorité	Conseil d'administration

Version	Date	Approuvée par
1.0	3 décembre 2024	Conseil d'administration
1.1	9 avril 2026	Conseil d'administration

1. Objet et champ d'application

Objet

La présente politique a pour objectif d'établir des lignes directrices et les procédures pour la gestion et l'alignement des ressources et activités informatiques sur les objectifs stratégiques de l'ACCPI. En adhérant à cette politique de gouvernance des TI et d'atténuation des risques, l'ACCPI assure la sécurité de son infrastructure informatique, le respect des exigences légales et la protection de ses données et ressources. Tous les employé(e)s sont tenu(e)s de comprendre et de respecter ces politiques, afin de contribuer à un environnement de travail sécuritaire et productif.

La présente politique vise à :

- Maintenir la sécurité et l'intégrité de l'infrastructure informatique de l'ACCPI
- Assurer la conformité aux exigences légales, réglementaires et sectorielles
- Soutenir la productivité en fournissant des lignes directrices claires sur l'utilisation des ressources informatiques
- Réduire les risques liés aux opérations informatiques, notamment les violations de données, les accès non autorisés et la perte d'équipement
- Décrire les procédures permettant de répondre efficacement aux incidents liés aux TI
- Assurer une prise de décision efficace et la création de valeur grâce à l'utilisation de la technologie

- Établir des normes de gouvernance pour la plateforme numérique intégrée IMMeSuite™ et tous les services technologiques destinés aux membres et exploités par l'ACCPI
- Assurer le déploiement responsable et la supervision des systèmes d'intelligence artificielle utilisés tant à l'interne que dans les services destinés aux membres

Champ d'application

La présente politique s'applique à tous les employé(e)s de l'ACCPI, notamment les employé(e)s à temps plein et à temps partiel, les directeurs/directrices et les bénévoles, les entrepreneur(e)s, les stagiaires, les consultant(e)s, les fournisseurs et fournisseuses tiers qui interagissent avec l'infrastructure informatique de l'organisation, ainsi que toute autre personne ayant accès aux ressources informatiques de l'ACCPI. Elle couvre l'ensemble des systèmes, réseaux, appareils, données et outils de communication informatiques appartenant à l'ACCPI, loués ou utilisés par elle, y compris ceux utilisés par les travailleurs et travailleuses à distance et les employé(e)s mobiles.

Application spécifique à IMMeSuite™ : La présente politique s'applique aux dix services IMMeSuite — IMMeMentor, IMMeForum, IMMeFile, IMMeEducation, IMMeCentre, IMMeLegal, IMMeSupport, IMMeJobs, IMMeAffiliate et IMMeMyConsultant — ainsi qu'au tableau de bord CAPIC Connect 2.0, au répertoire public MyConsultant.ca et à l'assistante intelligente AI Annie. Toutes les données collectées, traitées, stockées ou transmises par l'intermédiaire de ces plateformes sont assujetties aux dispositions de la présente politique et de la politique de confidentialité de l'ACCPI.

Traitement transfrontalier des données : lorsque les services IMMeSuite sont accessibles depuis l'extérieur du Canada, l'ACCPI s'assure que les renseignements personnels transférés d'une frontière à l'autre sont protégés selon une norme substantiellement similaire à celle de la loi canadienne sur la protection de la vie privée, conformément à la LPRPDE et à la législation provinciale applicable.

2. Exigences de sécurité

Sécurité des appareils

- Appareils personnels et fournis par l'entreprise : tous les appareils personnels et fournis par l'entreprise doivent être sécurisés conformément aux normes de sécurité de l'ACCPI, notamment par l'utilisation obligatoire d'un logiciel antivirus, de pare-feu et de mises à jour régulières.
- Antivirus et logiciel anti-maliciel : tous les appareils doivent être dotés d'un logiciel antivirus et anti-maliciel approuvé, configuré pour les mises à jour et les analyses automatiques.
- Correctifs et mises à jour : les appareils doivent être configurés pour les mises à jour automatiques afin que les derniers correctifs de sécurité soient appliqués rapidement.
- Sécurité physique : toutes les personnes visées doivent protéger les appareils contre le vol ou la perte en utilisant des verrous de sécurité, en maintenant les appareils sous surveillance et en les rangeant dans des armoires ou des tiroirs verrouillés lorsqu'ils ne sont pas utilisés.

Protection des données

- Traitement des données : toutes les personnes visées doivent traiter les données sensibles avec soin, en veillant à ce qu'elles soient stockées de façon sécurisée, chiffrées au besoin et accessibles uniquement au personnel autorisé.
- Chiffrement : les données sensibles doivent être chiffrées tant au repos qu'en transit, conformément aux normes de chiffrement approuvées par l'ACCPI.
- Partage sécurisé de fichiers : le partage de données doit s'effectuer par des canaux sécurisés (p. ex., services de partage de fichiers approuvés par l'ACCPI avec chiffrement de bout en bout).
- Destruction des données : des procédures adéquates de destruction des données doivent être respectées, notamment la suppression numérique et la destruction physique des supports de stockage.

2.2.1 Cadre de classification des données

Toutes les données des systèmes de l'ACCPI, y compris les services IMMeSuite, doivent être classées dans les catégories suivantes :

- Confidentiel : les renseignements personnels des membres, données financières, dossiers de clients, dossiers disciplinaires, documents du conseil d'administration tenus à huis clos et dossiers RH. Accès limité au personnel autorisé ayant un besoin démontré de connaître l'information.
- À l'interne : documents opérationnels, communications internes, rapports du personnel, projets de politiques, documents de comités et contenu modéré par IMMeForum. Accès réservé au personnel de l'ACCPI, aux directeurs et aux directrices, et aux bénévoles autorisé(e)s.
- Public : documents de politique publiés, listes du répertoire MyConsultant.ca, matériel de marketing et infolettres. Aucune restriction d'accès.

Les responsables des données ont la charge de classer les données relevant de leur domaine de service. Un registre de classification des données doit être tenu à jour et révisé annuellement.

Sécurité du réseau

- Connexions sécurisées : toutes les connexions réseau doivent être sécurisées au moyen de méthodes approuvées par l'ACCPI, telles que les réseaux privés virtuels (RPV ou VPN), disponibles exclusivement pour les personnes utilisant des appareils appartenant à l'ACCPI pour l'accès à distance. Les réseaux Wi-Fi publics doivent être évités à des fins professionnelles, sauf si la connexion passe par un RPV.
- Segmentation du réseau : le réseau de l'ACCPI est segmenté afin de restreindre l'accès conformément au principe du moindre privilège.
- Configuration des pare-feu : les pare-feu doivent être configurés pour protéger le réseau de l'ACCPI contre les accès non autorisés et faire l'objet d'une vérification régulière.

3. Contrôle d'accès

Authentification

- Politiques de mots de passe robustes : toutes les personnes visées doivent utiliser des mots de passe forts répondant aux exigences de complexité de l'ACCPI, notamment une longueur minimale, l'utilisation de caractères spéciaux et des mises à jour régulières.
- Authentification multifactorielle (MFA) : l'authentification multifactorielle est requise pour accéder à tous les systèmes et applications de l'ACCPI, offrant ainsi une couche de sécurité supplémentaire.
- Procédures de connexion sécurisées : toutes les personnes visées doivent suivre des procédures de connexion sécurisées, notamment se déconnecter des appareils lorsqu'ils ne sont pas utilisés et éviter les ordinateurs partagés ou publics pour accéder aux systèmes de l'ACCPI.

Autorisation

- Niveaux d'accès : les niveaux d'accès sont définis en fonction du rôle de la personne et du besoin de connaître, garantissant un accès uniquement aux informations nécessaires.
- Contrôle d'accès basé sur les rôles (CABR) : l'ACCPI utilise le CABR pour s'assurer que les personnes n'ont accès qu'aux données et aux systèmes nécessaires à l'exercice de leurs fonctions.
- Révisions périodiques des accès : les privilèges d'accès sont révisés périodiquement, afin de s'assurer qu'ils demeurent appropriés compte tenu des rôles et des responsabilités.

3.1 Gouvernance des accès IMMeSuite

L'accès aux fonctions administratives d'IMMeSuite doit respecter le principe du moindre privilège. Chaque secteur de service IMMeSuite est responsable de la gestion des accès des utilisateurs et utilisatrices dans son champ d'application. L'accès des membres aux services IMMeSuite est régi par le statut d'adhésion à l'ACCPI ; l'accès est automatiquement suspendu en cas de perte du statut de membre en règle, conformément au Règlement 2024-1, art. 2.8.

4. Utilisation des ressources de l'organisation

Matériel et logiciels

- Utilisation autorisée : toutes les personnes visées doivent utiliser les appareils et les logiciels fournis par l'entreprise exclusivement à des fins professionnelles. L'utilisation personnelle est restreinte et surveillée, afin d'assurer le respect de la présente politique.
- Installation de logiciels : le téléchargement ou l'installation de logiciels non autorisés est interdit pour prévenir les maliciels et l'utilisation de logiciels non autorisés. Toute installation de logiciel doit être approuvée par le service informatique.
- Entretien du matériel : toutes les personnes visées sont responsables de l'utilisation et de l'entretien adéquats du matériel fourni par l'entreprise et doivent signaler immédiatement tout problème ou dommage à la coordonnatrice administrative ou au coordonnateur administratif.

Soutien informatique

- Signalement des problèmes informatiques : le soutien informatique est accessible exclusivement par l'intermédiaire du sous-traitant informatique désigné par l'ACCPI. Pour obtenir de l'aide avec les ordinateurs portables, Office 365 ou d'autres préoccupations liées aux TI, telles que des défaillances matérielles, des erreurs logicielles ou des problèmes de sécurité, toutes les personnes visées doivent contacter rapidement le sous-traitant informatique. Tous les problèmes doivent être signalés à l'équipe informatique, afin d'en assurer la prise en charge efficace et la résolution rapide.

4.1 Approvisionnement en TI

L'acquisition de ressources informatiques – y compris les licences logicielles, les services infonuagiques, les abonnements SaaS, le matériel et les contrats avec des fournisseurs tiers – est soumise à la présente politique et à la politique d'approvisionnement de l'ACCPI. L'acquisition de ressources informatiques doit inclure une évaluation de sécurité documentée portant sur les pratiques de traitement des données, les normes de chiffrement, les contrôles d'accès et la conformité à la LPRPDE.

5. Outils et protocoles de communication

Outils approuvés

Toutes les communications professionnelles doivent utiliser des plateformes de communication et de collaboration approuvées par l'ACCPI. La liste des outils approuvés doit être tenue à jour et révisée annuellement. L'approbation de nouveaux outils de communication exige une évaluation documentée des fonctionnalités de sécurité, de la conformité à la présente politique et de la compatibilité avec les systèmes de l'ACCPI.

- Lignes directrices d'utilisation des outils : toutes les personnes visées doivent suivre les lignes directrices d'utilisation de chaque outil approuvé, notamment la configuration adéquate, la gestion des canaux de communication et le respect des paramètres de sécurité.
- IMMeForum est la plateforme désignée pour les discussions professionnelles entre membres, conformément à la Politique de communication de l'ACCPI.

Étiquette des communications

- Conduite professionnelle : toutes les personnes visées doivent maintenir une conduite professionnelle dans toutes leurs communications, conformément aux lignes directrices de l'ACCPI en matière de communication respectueuse et constructive.
- Délais de réponse : toutes les personnes visées sont tenues de répondre aux communications professionnelles dans les délais établis, afin d'assurer la collaboration et la productivité.

6. Politique d'utilisation de l'IA

6.1 Utilisation de l'IA par le personnel

L'utilisation des outils d'IA à l'ACCPI doit être conforme aux lignes directrices organisationnelles et avoir reçu une approbation préalable. Les outils d'IA sont réservés aux membres du personnel auxquels l'accès a été accordé. Ces outils ont pour but d'accroître la productivité, de simplifier

les flux de travail et de soutenir les objectifs de l'ACCPI, tout en assurant la conformité aux normes de confidentialité, de sécurité et d'éthique, ainsi que la non-discrimination. Ils ne doivent pas être utilisés pour prendre des décisions en matière d'emploi sans un examen et une approbation supplémentaire de l'ACCPI. Le personnel est tenu d'utiliser l'IA de manière responsable et uniquement aux fins approuvées par l'organisation.

6.2 Systèmes d'IA destinés aux membres (AI Annie)

L'ACCPI exploite AI Annie, une assistante intelligente intégrée à l'écosystème IMMeSuite. Les exigences de gouvernance suivantes s'appliquent à AI Annie et à tout futur système d'IA destiné aux membres :

- Transparence : AI Annie doit clairement se présenter comme une assistante IA dans toutes les interactions avec les membres.
- Exactitude et limites : les résultats fournis par AI Annie sont à titre informatif et d'appui. Elle ne doit pas formuler de conseils juridiques ni rendre d'avis réglementaires. Tous les résultats doivent être accompagnés de mises en garde appropriées.
- Données d'entrée : les données des membres utilisées par AI Annie sont soumises au cadre de classification des données et à la Politique de confidentialité de l'ACCPI.
- Supervision humaine : les modèles sous-jacents d'AI Annie et ses lignes directrices comportementales doivent faire l'objet d'une révision périodique. Toute modification substantielle de ses capacités requiert une autorisation appropriée.
- Garde-fous éthiques : AI Annie ne doit pas effectuer de discrimination fondée sur un motif interdit en vertu de la Loi canadienne sur les droits de la personne et ne doit pas être utilisée pour prendre ou recommander des décisions affectant le statut des membres.
- Piste d'audit : les interactions importantes d'AI Annie impliquant des données confidentielles doivent être consignées et conservées conformément au calendrier de conservation des données.

7. Productivité et rendement

Heures de travail

- Horaires de travail prévus : les employé(e)s doivent respecter leurs horaires de travail prévus et être disponibles pour les communications et les réunions pendant ces périodes. Tout écart doit être communiqué à leurs supérieur(e)s.
- Suivi du temps : les employé(e)s sont tenu(e)s de consigner avec précision leurs heures de travail à l'aide des outils de suivi du temps approuvés par l'ACCPI.

Suivi du rendement

- Outils de surveillance : l'ACCPI utilise divers outils pour surveiller la productivité et le rendement, notamment des logiciels de gestion de projets, des systèmes de suivi du temps et des rencontres régulières avec les superviseurs.
- Évaluations du rendement : des évaluations du rendement régulières seront effectuées pour évaluer la productivité, le respect des politiques et la contribution générale aux objectifs de l'équipe.

8. Formation et sensibilisation

Formation en sensibilisation à la sécurité

- Formation obligatoire : toutes les personnes visées doivent suivre la formation obligatoire de sensibilisation à la cybersécurité lors de leur intégration et à intervalles réguliers par la suite.
- Formation continue : l'ACCPI offre des possibilités de formation continue sur les meilleures pratiques en matière de cybersécurité, notamment la prévention, le traitement sécurisé des données et la réponse aux incidents.

Exigences de formation étendues (mars 2026) :

- Fréquence : la formation doit être complétée annuellement. Le nouveau personnel doit terminer la formation dans les 30 jours suivant le début de ses fonctions.
- Contenu : protection des données et obligations en vertu de la LPRPDE ; sécurité des appareils et du réseau ; sensibilisation à l'honnêteté ; signalement des incidents ; lignes directrices sur l'utilisation de l'IA ; traitement des données propre à la plateforme IMMeSuite ; et Code de conduite de l'ACCPI en matière de sécurité de l'information.
- Suivi de la conformité : l'achèvement de la formation doit être suivi et communiqué régulièrement, afin d'assurer la conformité organisationnelle.
- Formation spécialisée : le personnel ayant un accès administratif aux services sensibles d'IMMeSuite doit recevoir une formation supplémentaire sur la gestion des données confidentielles des membres, dispensée au moins une fois par an.
- Directeurs/directrices et bénévoles : ils/elles doivent recevoir un résumé de sensibilisation à la sécurité au début de chaque mandat au conseil d'administration ou de chaque nomination à titre de bénévole.

Accusé de réception de la politique

- Procédure d'accusé de réception : toutes les personnes visées doivent accuser réception de la politique informatique et confirmer leur compréhension et leur conformité lors de leur intégration et à chaque mise à jour de la politique. Le non-respect de cette obligation peut entraîner un accès restreint aux systèmes de l'ACCPI.

9. Conformité et considérations juridiques

Conformité réglementaire

- Lignes directrices de conformité : toutes les personnes visées doivent se conformer à toutes les lois et règlements pertinents, tels que le RGPD, la LPRPDE et les exigences sectorielles, afin d'assurer la conformité et d'éviter les sanctions juridiques.
- Audits et évaluations : des audits et des évaluations réguliers sont effectués pour assurer la conformité aux exigences réglementaires et aux politiques internes de l'ACCPI.

Protection de la vie privée

- Politiques de confidentialité : les politiques de confidentialité des données de l'ACCPI doivent être respectées pour protéger les données personnelles et organisationnelles, en assurant la confidentialité et la gestion adéquate des violations et des incidents de perte de données.
- Notification d'une violation : en cas de violation de données, l'ACCPI avisera les parties concernées comme l'exige la loi et prendra des mesures pour atténuer les effets de la violation.

10. Révision et mises à jour

Révision régulière

- Calendrier de révision : la politique informatique sera révisée annuellement, ou plus fréquemment si des changements dans le paysage des menaces, les exigences réglementaires ou les pratiques commerciales le nécessitent.
- Mises à jour de la politique : les mises à jour de la politique seront communiquées à toutes les personnes visées, qui devront accuser réception et confirmer leur compréhension des modifications.

Rétroaction des employés

- Mécanisme de rétroaction : les employé(e)s sont invité(e)s à formuler des commentaires sur la politique informatique par les canaux de rétroaction désignés, notamment des sondages ou des communications directes avec l'équipe de gouvernance des TI.
- Amélioration continue : les commentaires seront examinés régulièrement, et les améliorations proposées seront prises en compte lors des prochaines mises à jour de la politique.

11. Usage personnel et vie privée

Utilisation d'appareils personnels

- Lignes directrices d'utilisation : les employé(e)s sont autorisé(e)s à utiliser des appareils personnels à des fins professionnelles uniquement s'ils respectent les normes de sécurité de l'ACCPI, notamment en installant les logiciels de sécurité approuvés et en chiffrant les données.
- Restrictions : les appareils personnels ne doivent pas servir à stocker des données organisationnelles sensibles. Toutes les données professionnelles doivent être stockées sur des appareils approuvés par l'entreprise ou sur un stockage infonuagique sécurisé.

Attentes en matière de vie privée

- Politique de surveillance : l'ACCPI surveille les activités professionnelles, y compris l'utilisation des ressources informatiques, afin d'assurer le respect des politiques et de protéger les biens de l'organisation. Les employé(e)s ne doivent pas s'attendre à la confidentialité lorsqu'ils utilisent les ressources de l'entreprise.

- Collecte de données : les données de surveillance seront collectées et stockées de manière sécurisée, avec un accès limité au seul personnel autorisé.

12. Sanctions en cas de non-conformité

Conséquences

- Mesures disciplinaires : le non-respect de la présente politique informatique peut entraîner des mesures disciplinaires, notamment des avertissements, une suspension ou une cessation d'emploi, selon la gravité de la violation.
- Conséquences juridiques : les employé(e)s peuvent également faire face à des conséquences juridiques en cas de violation de la confidentialité, des lois sur la protection des données ou d'autres exigences réglementaires.
- Les fournisseurs tiers peuvent faire l'objet d'une résiliation de contrat et de poursuites judiciaires s'ils ne respectent pas la présente politique.

13. Instructions d'intégration

Préparation avant l'arrivée

- Configuration du compte informatique : avant la date d'entrée en fonction du nouvel employé ou d'une nouvelle employée, le service informatique créera les comptes utilisateurs, configurera les permissions d'accès et préparera les appareils.
- Provisionnement du matériel : les appareils et les logiciels nécessaires seront préinstallés et configurés conformément aux exigences de sécurité.

Intégration le premier jour

- Séance d'information sur la sécurité : Les nouveaux employés et les nouvelles employées recevront une séance d'information sur la sécurité couvrant les politiques clés, notamment la sécurité des appareils, le traitement des données et les procédures de signalement des incidents.
- Provisionnement des accès : les employé(e)s recevront leurs identifiants de connexion et seront guidés dans la configuration de l'authentification multifacteur (AMF) et d'autres mesures de sécurité.

Formation et ressources

- Formation sur les politiques : les employé(e)s suivront une formation sur les politiques informatiques, afin de comprendre toutes les exigences de sécurité, les contrôles d'accès et les politiques d'utilisation acceptable.
- Accès aux ressources : les employé(e)s auront accès à toutes les ressources nécessaires, notamment l'intranet des employé(e)s, les outils de collaboration et les coordonnées du soutien informatique.

14. Sécurisation des biens informatiques de l'ACCPI lors de départs ou d'absences d'employé(e)s

Procédures préalables au départ

- Notification et planification : les RH informeront le service informatique à l'avance des départs ou des absences prolongées, et une évaluation des risques sera effectuée pour déterminer les mesures de sécurité nécessaires.
- Sauvegarde des données : les données seront sauvegardées ou transférées au personnel autorisé pour prévenir toute perte de données.

Actions immédiates lors d'un départ

- Désactivation des comptes : tous les comptes utilisateurs et les privilèges d'accès à distance seront immédiatement désactivés.
- Récupération des appareils : tous les appareils fournis par l'entreprise seront collectés, inspectés et effacés de façon sécurisée pour supprimer toutes les données.

Procédures post-départ

- Fermeture permanente des comptes : les comptes utilisateurs seront définitivement supprimés ou archivés conformément aux exigences de la politique.
- Modification des identifiants : tous les mots de passe et identifiants partagés accessibles par l'employé(e) démissionnaire seront modifiés.

Gestion des absences prolongées

- Suspension des comptes : les comptes seront temporairement suspendus pendant les absences prolongées, l'accès étant rétabli au retour.
- Sécurité des appareils : les appareils non utilisés seront stockés en toute sécurité, et les droits d'accès seront revus et ajustés si nécessaire.

Communication et documentation

- Protocole de communication : Une communication claire entre les RH, le service informatique et le gestionnaire ou la gestionnaire de l'employé(e) sera maintenue pour s'assurer que les procédures adéquates sont suivies.
- Documentation : toutes les actions effectuées lors d'un départ ou d'une absence seront documentées dans une liste de vérification de fin d'emploi et un rapport d'incident si nécessaire.

Considérations juridiques et de conformité

- Examen juridique : toutes les procédures seront conformes aux lois pertinentes et aux politiques de l'ACCPI, assurant la conformité juridique et réglementaire.
- Conservation des données et vie privée : les données seront traitées conformément aux politiques de conservation des données de l'ACCPI, dans le respect des droits à la vie privée.

15. Gestion des risques liés aux fournisseurs et aux tiers

Tous les fournisseurs tiers, prestataires de services et partenaires technologiques qui accèdent aux données de l'ACCPI, les traitent, les stockent ou les transmettent sont soumis aux exigences suivantes :

- Évaluation de sécurité des fournisseurs : avant tout engagement, les fournisseurs doivent démontrer leur conformité aux normes de traitement des données, de chiffrement et de contrôle d'accès de l'ACCPI, ainsi qu'aux lois canadiennes applicables en matière de protection de la vie privée.
- Ententes de traitement des données : Tous les fournisseurs traitant des données de membres de l'ACCPI doivent signer une entente écrite de traitement des données précisant les utilisations autorisées, les obligations de sécurité, les délais de notification des violations et le retour ou la destruction des données à la fin du contrat.
- Obligations des partenaires : les partenaires du programme d'affinité qui reçoivent ou consultent des données de membres doivent se conformer aux normes de protection des données énoncées dans leurs ententes respectives.
- Surveillance continue : la conformité des fournisseurs doit être vérifiée régulièrement. Les incidents de sécurité importants chez les fournisseurs doivent être signalés et traités rapidement.

16. Réponse aux incidents

Un incident de sécurité informatique est tout événement qui compromet ou menace la confidentialité, l'intégrité ou la disponibilité des systèmes, des données ou des services informatiques de l'ACCPI, y compris ceux qui soutiennent IMMeSuite. Cela inclut les accès non autorisés, les violations de données, les infections par des logiciels malicieux, les interruptions de service et les dysfonctionnements des systèmes d'IA.

- Tout incident présumé doit être signalé immédiatement au contact informatique désigné.
- Les incidents doivent être évalués en fonction de leur gravité et traités rapidement, les mesures de confinement, d'enquête et de correction étant documentées.
- Les incidents importants doivent faire l'objet d'un examen post-incident identifiant la cause profonde et permettant d'améliorer les politiques.
- Lorsqu'une violation de renseignements personnels crée un risque réel de préjudice grave, l'ACCPI doit remplir ses obligations de notification en vertu de la LPRPDE.

17. Continuité des activités et reprise après sinistre

L'ACCPI doit maintenir un Plan de continuité des activités (PCA) et un Plan de reprise après sinistre (PRS) pour son infrastructure informatique, y compris tous les services IMMeSuite. Le PCA/PRS doit être révisé et testé au moins une fois par an.

- Sauvegarde des données : toutes les données de l'ACCPI doivent être sauvegardées régulièrement. Les sauvegardes doivent être chiffrées, stockées séparément des systèmes primaires et testées quant à leur récupérabilité.

- Objectifs de rétablissement : des objectifs de temps de rétablissement et de point de récupération doivent être établis pour chaque service critique, classés par ordre de priorité selon l'impact sur les membres.
- Plan de communication : le PCA doit inclure un plan de communication pour les pannes prolongées utilisant des canaux indépendants des systèmes affectés.
- Tests annuels : au moins un exercice de reprise doit être effectué annuellement, les résultats étant documentés et utilisés pour améliorer le plan.

18. Supervision de la gouvernance et responsabilité

- Supervision et responsabilité : l'ACCPI assure une supervision continue de son cadre de gouvernance des TI, afin de garantir que les pratiques de sécurité, de conformité et de gestion des risques sont respectées dans l'ensemble de ses systèmes, plateformes et services.
- Alignement des politiques : la présente politique sera révisée selon un cycle régulier et doit être lue conjointement avec toutes les politiques connexes de l'ACCPI, notamment les politiques de confidentialité, de communication, d'approvisionnement, de conflits d'intérêts et de code de conduite et d'éthique.

Approbation

Approuvée par le conseil d'administration de l'Association canadienne des consultants professionnels en immigration (CAPIC–ACCPI).

Approuvée initialement	Approuvée
3 décembre 2024	9 avril 2026