Politique : Politique de protection de la vie privée
Sous-section : Finances
Date de la dernière révision : Nouvelle politique
Date de la dernière approbation : Le 25 juin 2024

1. But

Le but de la présente politique est le suivant :

- Définir ce que sont les Renseignements permettant d'identifier une personne (RPIP) et établir des normes quant à la façon dont le personnel, les sous-traitants, les fournisseurs et les partenaires du CPC doivent les recueillir, les tenir à jour, les conserver et les détruire.

2. Inclusion, diversité, équité et accessibilité

La présente politique a été évaluée en fonction des incidences qu'elle pourrait avoir sur l'inclusion, la diversité, l'équité et l'accessibilité.

3. Portée de la politique

La présente politique couvre l'intégralité des activités et services du Comité paralympique canadien.

4. Responsabilités

Les responsabilités du **conseil d'administration** sont les suivantes :

4.1 Mettre en place et approuver des politiques et des lignes directrices; et

4.2 Veiller à ce que les pratiques en matière de protection de la vie privée concordent avec les exigences légales et réglementaires

Les responsabilités du **Comité des finances, de la vérification et des risques (FVR)** sont les suivantes :

4.3 Rendre compte au conseil d'administration de la performance du CPC en matière de protection de la vie privée et du respect, par le CPC, des lois et règlements connexes; et

4.4 Évaluer et gérer les risques liés au respect de la vie privée

Les responsabilités de **l'équipe dirigeante** sont les suivantes :

4.5 Établir, mettre en œuvre et maintenir de bonnes pratiques en matière de protection de la vie privée dans tous les secteurs de l'organisation, y compris en donnant l'exemple;

4.6 Fournir les ressources nécessaires à la mise en œuvre de mesures appropriées et veiller au respect de la politique;

4.7 Fournir aux employés, à intervalles réguliers, des possibilités de formation sur la protection de la vie privée; et

4.8 Veiller à ce que les contrats avec les fournisseurs contiennent des exigences en matière de sécurité et de protection de la vie privée.

Les responsabilités des **employés** sont les suivantes :

4.9 Adhérer aux lignes directrices et aux procédures établies en matière de protection de la vie privée;

4.10 Signaler rapidement toute inquiétude ou tout incident potentiel en matière de protection de la vie privée; et

4.11 Utiliser des mots de passe complexes, des dispositifs de cryptage et des canaux sécurisés pour la transmission de données.

5. Définitions

5.1 Les **Renseignements permettant d'identifier une personne (RPIP)** comprennent tous les renseignements factuels ou subjectifs, enregistrés ou non, à propos d'une personne identifiable. Cela comprend, entre autres, les renseignements suivants, quelle qu'en soit la forme :

- âge, nom, adresse, numéro de téléphone, code postal, numéros de pièce d'identité, revenu, origine ethnique ou groupe sanguin;
- opinions, évaluations, commentaires, statut social ou mesures disciplinaires;

- dossiers d'employé(e), dossiers de crédit, dossiers de prêt, dossiers médicaux, existence d'un différend entre un consommateur et un commerçant, intentions (par exemple, d'acheter des biens ou des services, ou de changer d'emploi); et
- tout type de données médicales

6. Limitations

7. Contenu de la politique

7.1 Collecte de RPIP

Le personnel, les sous-traitants, les fournisseurs et les partenaires du CPC ne doivent pas recueillir de RPIP, sauf si les circonstances opérationnelles l'exigent clairement. L'équipe dirigeante doit approuver toute collecte de RPIP ne relevant pas des exigences opérationnelles avant d'entamer ladite collecte.

7.2 Conservation et tenue à jour des RPIP

Les RPIP doivent être cryptés au moyen d'une clé de chiffrement d'au moins 128 bits chaque fois qu'ils sont en transit et au repos. Seuls les utilisateurs autorisés doivent avoir accès au système ou à la base de données de RPIP, et uniquement pendant la période au cours de laquelle leurs activités requièrent cet accès. Tous les systèmes permettant d'accéder aux RPIP doivent être sécurisés au moyen d'une authentification multifactorielle et feront l'objet d'audits d'accès trimestriels.

7.3 Droit à l'oubli

Le CPC maintiendra la capacité à fournir aux individus le « droit à l'oubli ». Le CPC mettra en place une procédure pour traiter les demandes de personnes souhaitant que leurs RPIP soient complètement effacés de ses systèmes. Le CPC mettra les détails de la procédure à la disposition du public via la Politique de protection de la vie privée.

7.4 Destruction

Si le stockage des RPIP ne répond plus à l'objectif opérationnel pour lequel ils ont été recueillis initialement, ils seront détruits. Les données peuvent être conservées sous forme agrégée.

7.5 Toute violation de la présente politique, en tout ou en partie, peut donner lieu à des mesures disciplinaires pouvant inclure, sans s'y limiter, la résiliation de l'emploi ou du contrat et/ou toute autre action en justice justifiée par les circonstances. Veuillez vous référer à la Politique disciplinaire du CPC pour de plus amples renseignements.

8. Documents/dossiers connexes

Politique sur la GI et Politique relative aux TI
Politique de gestion des risques

9. Historique des révisions