

Politique relative à l'utilisation de l'information figurant sur les cartes de crédit des clients

Justifications et liens avec notre mission, nos principes et nos valeurs

La Société canadienne de la sclérose en plaques (« Société de la SP ») est un organisme national de bienfaisance qui œuvre dans le domaine de la santé et qui est largement tributaire d'une variété d'activités de collecte de fonds en ce qui a trait à l'accomplissement de sa mission. Chaque année, des centaines de milliers de sympathisants de la Société de la SP font des dons par Internet ou par d'autres moyens dans le cadre du Vélo SP, de la Marche SP et de la campagne #stopponslaSP, que ce soit à titre individuel ou en équipe. Par conséquent, les employés, les contractuels et les bénévoles de l'organisme sont amenés à traiter un très grand volume de renseignements particulièrement sensibles, à savoir l'information figurant sur les cartes de crédit des donateurs. C'est pourquoi la Société de la SP a recours à un serveur crypté pour le traitement des dons qu'elle reçoit en ligne.

En plus de devoir appliquer ses propres directives visant à protéger la confidentialité et la sécurité des renseignements qui lui sont confiés, la Société de la SP est tenue de satisfaire à un certain nombre d'exigences légales et techniques. Sa Politique de protection de la vie privée et de la confidentialité et les procédures qui s'y rattachent lui permettent de garantir le respect des exigences établies par la loi dans ce domaine. En ce qui concerne le traitement des transactions par carte de crédit, notre organisme a pour obligation de satisfaire à des normes techniques fixées par le contrat qui le lie à son institution financière, laquelle a adhéré à une série de normes communément appelées « normes de sécurité sur les données de l'industrie des cartes de paiement » (dites également « normes PCI »).

Dans les faits, la Société de la SP a recours à des systèmes automatisés ainsi qu'à des procédés manuels pour traiter l'information figurant sur les cartes de crédit. Comme la majeure partie de nos revenus est attribuable à nos activités de collecte de fonds, il est primordial que la Société de la SP se conforme aux normes PCI afin de pouvoir poursuivre sa mission. Les sanctions à envisager en cas de non-conformité à cet ensemble de normes comprennent notamment 1) une augmentation des frais de transaction par carte de crédit, 2) une suspension des privilèges liés à l'utilisation de cartes de crédit et 3) l'application d'une amende dans les cas de fraude concernant un compte. Chacune de ces pénalités peut compromettre notre capacité à accomplir notre mission et nuire à la crédibilité de la Société de la SP auprès du public.

Objectif de la politique

La présente politique décrit les pratiques appropriées à adopter au sein de la Société de la SP relativement au traitement des transactions par carte de crédit effectuées à l'aide d'un système automatisé ou suivant un procédé manuel. Ce document fixe un certain nombre d'exigences dont l'objectif est de faire en sorte que l'information figurant sur les cartes de crédit soit utilisée, puis éliminée conformément à l'obligation qu'a la Société de la SP de protéger de tels renseignements d'une manière qui satisfait aux exigences de l'industrie des cartes de paiement ou les dépasse.

Comme la visibilité non autorisée de renseignements figurant sur une carte de crédit pourrait porter atteinte à la réputation de la Société de la SP et exposer celle-ci à des pénalités non négligeables, le défaut de se conformer à la présente politique et aux procédures qui s'y rattachent sera considéré comme une faute grave.

Champ d'application

Cette politique s'applique à :

- toute personne qui, au nom de la Société de la SP, accepte, saisit, stocke, transmet ou gère de l'information relative à des paiements faits par carte de crédit pour l'achat de produits ou de services de la Société de la SP, pour l'inscription à un événement de collecte de fonds proposé par la Société de la SP (p. ex. Vélo SP, Marche SP), pour l'apport d'une contribution sous la forme d'un don à la Société de la SP, ou pour toute autre activité approuvée par la Société de la SP et nécessitant l'utilisation de renseignements figurant sur une carte de crédit;
- toute personne qui peut être appelée à intervenir dans les opérations consistant – au sein de la Société de la SP – à accepter, à saisir, à stocker, à transmettre ou à gérer de l'information relative à des paiements faits par carte de crédit. Sont notamment concernés les employés du Service du soutien technique qui, dans l'exercice de leurs fonctions, ont accès aux ordinateurs et aux logiciels utilisés pour stocker l'information figurant sur les cartes de crédit, les personnes qui sont chargées de déchiqueter des documents comportant des renseignements figurant sur des cartes de crédit et celles dont le travail implique l'utilisation de ce type d'information.

Guide des politiques de la Société canadienne de la sclérose en plaques	
<i>S'applique à :</i>	Bénévoles et personnel de tous les échelons
<i>Fréquence des révisions :</i>	Annuelle
<i>Première approbation :</i>	12 décembre 2013 par le conseil d'administration de la Société canadienne de la SP
<i>Dernière révision :</i>	Mars 2021
<i>Prochaine révision :</i>	Mars 2022

Approbation

Cette politique a été approuvée par le conseil d'administration de la Société de la SP le 12 décembre 2013.

Détails

L'équipe de la haute direction est autorisée à élaborer des procédures détaillées pour l'application des directives énoncées dans cette politique au plus tard six mois après l'approbation de celle-ci.

1.0 Principes directeurs

- 1.1 La conformité aux normes PCI est obligatoire pour tous les échelons de l'organisme en ce qui a trait aux opérations suivantes : acceptation, saisie, stockage, transmission et gestion des renseignements figurant sur les cartes de crédit.
- 1.2 La formation des personnes appelées à gérer les renseignements figurant sur les cartes de crédit doit être assurée au moins deux fois par année. Le contenu du programme à offrir à ce chapitre doit être conforme aux modalités établies en matière de formation par les procédures qui se rattachent à la présente politique.
- 1.3 Seules les personnes autorisées et dûment formées peuvent accepter des renseignements figurant sur des cartes de crédit ou de débit ou accéder à ce type d'information.
- 1.4 Les paiements par carte de crédit peuvent être acceptés seulement s'ils sont effectués suivant une méthode approuvée par les services d'entreprise de la Société de la SP.
- 1.5 Toute personne ayant accès à des renseignements figurant sur des cartes de crédit a pour responsabilité de protéger cette information conformément à la Politique de protection de la vie privée et de la confidentialité en vigueur à la Société de la SP.
- 1.6 Les renseignements relatifs aux cartes de crédit doivent être détruits de manière sécuritaire immédiatement après leur utilisation, et ce, conformément aux modalités énoncées dans la Politique de protection de la vie privée et de la confidentialité en vigueur à la Société de la SP.
- 1.7 Les services doivent disposer d'un système approprié de contrôle et de vérification applicable à l'utilisation des renseignements figurant sur les cartes de crédit.
- 1.8 En vue de se conformer à la présente politique ainsi qu'aux normes PCI, les services qui utilisent les renseignements figurant sur des cartes de crédit doivent suivre les procédures documentées pertinentes, soit

Guide des politiques de la Société canadienne de la sclérose en plaques	
<i>S'applique à :</i>	Bénévoles et personnel de tous les échelons
<i>Fréquence des révisions :</i>	Annuelle
<i>Première approbation :</i>	12 décembre 2013 par le conseil d'administration de la Société canadienne de la SP
<i>Dernière révision :</i>	Mars 2021
<i>Prochaine révision :</i>	Mars 2022

celles que le Service national des finances a établies à ce chapitre pour l'ensemble de l'organisme.

- 1.9 Qu'il soit réel ou présumé, tout vol ou perte de renseignements relatifs à une carte de crédit doit être rapporté immédiatement au vice-président des services d'entreprise, au vice-président de la collectivité, au directeur principal de la collectivité, ainsi qu'à la personne responsable en matière de confidentialité.

Le défaut de se conformer aux principes directeurs susmentionnés pourrait aboutir au retrait de l'autorisation de traiter des transactions par carte de crédit ou à la prise de mesures disciplinaires (y compris la cessation de fonctions). Ces deux catégories de sanctions pourraient également être appliquées conjointement.

Maître d'œuvre

Le vice-président des services d'entreprise est le maître d'œuvre de la présente politique.

Surveillance et conformité

Le vice-président des services d'entreprise a pour responsabilité de s'assurer que des vérifications de conformité sont effectuées chaque année, de façon aléatoire, par des intervenants internes et des tiers dûment formés.

Le vice-président des services d'entreprise et le vice-président de la collectivité sont chargés de passer en revue les activités de la Société de la SP et de faire part de leurs observations au président et chef de la direction, tous les trois mois, en ce qui a trait à la conformité à la présente politique.

Politiques et lois connexes

- Conseil des normes de sécurité PCI (<http://fr.pcisecuritystandards.org/minisite/en/>)
- Politique et procédures relatives à la protection de la vie privée et de la confidentialité en vigueur à la Société de la SP
- Dispositions relatives à la sécurité des technologies de l'information établies par la Société de la SP
- Procédure de conservation des dossiers adoptée par la Société de la SP

Guide des politiques de la Société canadienne de la sclérose en plaques	
<i>S'applique à :</i>	Bénévoles et personnel de tous les échelons
<i>Fréquence des révisions :</i>	Annuelle
<i>Première approbation :</i>	12 décembre 2013 par le conseil d'administration de la Société canadienne de la SP
<i>Dernière révision :</i>	Mars 2021
<i>Prochaine révision :</i>	Mars 2022

Révision

Cette politique doit être passée en revue au moins tous ans suivant son approbation conformément aux normes PCI.

Définitions

Équipe de la haute direction – Groupe d’employés occupant les postes de direction les plus élevés de la Société de la SP, soit le président et chef de la direction, les présidents, les vice-présidents principaux et les vice-présidents. Ces personnes peuvent cumuler plusieurs postes. Le président et chef de la direction peut modifier la composition de l’équipe de la haute direction, au besoin.

Bureau national – Organe qui coordonne le travail de la Société de la SP dans son ensemble. Il a pour mandat d’assurer la supervision stratégique de l’organisme et de veiller à la diffusion des pratiques exemplaires dans toutes les sphères d’activité. Le Bureau national est chargé de gérer le programme de recherche et les programmes de marketing direct, d’assurer la centralisation des processus financiers ainsi que d’administrer une plateforme centralisée de technologie de l’information.

Normes de sécurité sur les données de l’industrie des cartes de paiement (« Normes PCI ») – Afin de réduire leurs pertes attribuables aux fraudes liées aux cartes de crédit, les membres de l’industrie des cartes de paiement ont uni leurs efforts pour élaborer des normes de sécurité applicables aux entreprises et aux organismes qui acceptent, saisissent, stockent, transmettent ou gèrent de l’information relative à des cartes de crédit, que ce soit manuellement ou au moyen d’un système automatisé. Cet ensemble de normes est également désigné « normes PCI ».

Guide des politiques de la Société canadienne de la sclérose en plaques	
<i>S’applique à :</i>	Bénévoles et personnel de tous les échelons
<i>Fréquence des révisions :</i>	Annuelle
<i>Première approbation :</i>	12 décembre 2013 par le conseil d’administration de la Société canadienne de la SP
<i>Dernière révision :</i>	Mars 2021
<i>Prochaine révision :</i>	Mars 2022