| NOM DE LA POLITIQUE | POLITIQUE RELATIVE À L'ACCEPTATION DE PAIEMENTS PAR CARTE DE CRÉDIT OU DE DÉBIT APPLICABLE AUX COMMERÇANTS |
|---|---|
| **Version** | V1.6 |
| **Date de publication** | 11 août 2009 |
| **Date de révision** | 8 mars 2023 |
| **Date d'entrée en vigueur** | 8 mars 2023 |

## OBJET ET PORTÉE

De nombreuses unités de l'Université stockent, traitent ou transmettent des données de titulaires de carte de crédit, de débit ou prépayée utilisées pour l'achat de biens ou de services ou le versement de dons. Ces paiements doivent respecter la norme de sécurité des données du secteur des cartes de paiement, désignée par le sigle PCI DSS. Cette norme a pour but de protéger les données des titulaires de cartes de crédit, de débit ou prépayées lors du traitement et de la transmission des transactions.

L'Université est tenue d'obtenir une attestation de conformité de ses systèmes et processus à la norme PCI DSS pour traiter des transactions par carte de paiement. Étant donné que cette attestation s'applique à l'ensemble de l'établissement, les commerçants doivent respecter les normes énoncées dans la présente politique. Tout manquement peut entraîner :

- un risque accru de transactions frauduleuses portées au compte des titulaires de carte;
- une baisse de la qualité du service à la population étudiante et diplômée et au grand public;
- des amendes;
- une atteinte à la réputation de l'Université;
- le retrait de l'attestation de conformité, qui empêche alors l'Université d'accepter les paiements par carte de crédit, de débit ou prépayée.

Les dispositions relatives à l'application et à l'interprétation de la présente politique sont énoncées à la rubrique Procédures.

# PORTÉE

La présente politique s'applique à l'ensemble des membres du personnel de l'Université qui acceptent et traitent des paiements par carte de crédit, de débit ou prépayée, ou qui fournissent les infrastructures nécessaires pour ces transactions. Les membres du personnel doivent s'assurer que toute autre partie (membre de la population étudiante, bénévole, fournisseur) respecte la présente politique. Les entités indépendantes de McGill qui utilisent son nom doivent également s'y conformer. Le non-respect de la politique peut entacher le nom et la réputation de McGill et entraîner le retrait de son attestation de conformité. Aux fins de la présente politique, « membre du personnel » s'applique à l'ensemble du personnel enseignant, administratif et de recherche.

Seules les unités que l'Université (Services financiers) reconnaît comme des « commerçants » peuvent accepter et traiter les paiements par carte de crédit, de débit ou prépayée. Quel que soit le mode de paiement utilisé, tous les commerçants doivent respecter la présente politique.

**Commerce électronique**
Les titulaires de carte qui paient un achat ou versent un don en ligne doivent saisir le numéro, la date d'expiration et le code de vérification de la carte.

**Pointes de vente**
Les points de vente utilisent les terminaux des fournisseurs de traitement des paiements de l'Université pour le règlement des achats en présence des titulaires de carte. La transaction est confirmée lorsque le commerçant reçoit un code d'autorisation.

**Système de réponse vocale interactive**
Les commerçants qui ne disposent pas d'une solution de paiement électronique ni d'un terminal peuvent obtenir un code d'autorisation en saisissant le numéro et la date d'expiration de la carte dans le système téléphonique automatisé du fournisseur de traitement des paiements. Si la ou le titulaire de la carte est présent, le commerçant lui remet une preuve de paiement imprimée.

# POLITIQUE

## P1.

Tous les commerçants de l'Université doivent respecter la présente politique. Les commerçants qui ne se conforment pas à la politique à la satisfaction du Comité directeur sur la conformité aux normes PCI se verront retirer le droit de traiter les paiements par carte.

## P2. Comptes marchands

Avant de pouvoir traiter les paiements par carte (pour l'achat de biens ou de services ou le versement de dons), l'unité doit obtenir un compte marchand approuvé par l'Université. Les Services financiers sont la **seule** unité administrative autorisée à créer ces comptes; par conséquent, les commerçants qui traitent des paiements par carte en ligne, au point de vente ou par le système téléphonique automatisé doivent obtenir **l'autorisation écrite préalable** des Services financiers, afin que:

- toutes les transactions par carte de crédit, de débit ou prépayée soient traitées par les fournisseurs de traitement des paiements de l'Université;
- toutes les recettes soient déposées dans un compte bancaire central de l'Université approuvé par les Services financiers.

## P3. Comptes bancaires

Les unités ne sont pas autorisées à ouvrir un compte bancaire ou tout autre type de compte commercial (p. ex., Paypal) au nom de l'Université. Seuls les Services financiers peuvent établir des comptes bancaires commerciaux au nom de l'Université.

## P4. Norme de sécurité des données du secteur des cartes de paiement (PCI DSS)

Toutes les transactions par carte de crédit, de débit ou prépayée doivent être conformes à la norme PCI DSS, faute de quoi l'Université se verra retirer le droit de traiter les paiements par carte. Les unités doivent respecter toutes les exigences énoncées par le Comité directeur sur la conformité aux normes PCI.

**P5.**

Il est interdit de stocker les données des titulaires de carte sur un support électronique (feuille de calcul, lecteur de réseau, serveur de base de données) et de les transmettre par voie électronique (courriel, messagerie instantanée) ni par VoIP (Voix sur IP).

## P6. Conservation et élimination des documents justificatifs

Les transactions financières doivent être étayées par des pièces justificatives, par exemple un reçu ou une facture indiquant l'objet du paiement et le nom de la personne qui l'a effectué. Ces pièces justificatives sont à conserver selon les règles de l'Université, en général pour une durée de sept ans.

Il n'est pas nécessaire de conserver les confirmations de paiement (reçus ou impressions), puisque la transaction apparaît dans le relevé bancaire de l'Université, sauf si les données des titulaires de carte sont indiquées sur les confirmations. Le cas échéant, celles-ci doivent être conservées en lieu sûr (dans un endroit sous clé dont l'accès est réservé au personnel autorisé) durant 18 mois, à la seule fin du règlement d'un éventuel litige. Les confirmations doivent être détruites immédiatement à la fin de ce délai.

Les commerçants doivent configurer leurs gabarits de sorte que les renseignements des cartes de paiement n'apparaissent pas sur les documents auxquels de nombreuses personnes ont accès ou qui doivent être conservés sur une longue période. Les anciens documents considérés comme des pièces justificatives qui contiennent une confirmation de paiement indiquant les renseignements de la carte utilisée doivent être conservés uniquement sur un support papier dans un lieu dont l'accès est réservé aux personnes autorisées. Dans des circonstances exceptionnelles et avec l'accord par écrit du Comité directeur sur la conformité aux normes PCI, des données de titulaires de carte de paiement peuvent être conservées sur un support électronique dans un répertoire autorisé.

## P7. Solutions

Tout logiciel développé par McGill et toute solution tierce qui stocke, traite ou transmet des informations relatives aux cartes de crédit, ou qui pourrait avoir un impact sur la sécurité des données des titulaires de cartes, doivent être évalués et approuvés par le Comité directeur sur la conformité aux normes PCI, McGill étant contractuellement tenue d'obtenir l'approbation de son acquéreur.

La conformité PCI doit être intégrée à tout processus d'appel d'offres public.

## P8. Signalement d'incidents

Tout incident relatif à la sécurité des données d'une ou d'un titulaire de carte de paiement doit être signalé immédiatement à la superviseure ou au superviseur des Services bancaires des Services financiers.

Les Services financiers en informent à leur tour les Services des technologies de l'information, selon les protocoles établis.

## P9. Gestion du changement

Toute modification à un processus, à un système, à des infrastructures ou à une application susceptible de modifier les renseignements déclarés au Comité directeur sur la conformité aux normes PCI (le questionnaire a l'intention des commerçants ou le questionnaire d'autoévaluation de la conformité à la norme PCI DSS) doit être signalée immédiatement à la superviseure ou au superviseur des Services bancaires des Services financiers.

# PROCÉDURES

## PR1. Comité directeur sur la conformité aux normes PCI

**PR1.1.**

Le Comité directeur sur la conformité aux normes PCI se fonde sur les pratiques exemplaires et les évaluations des risques de la PCI. Il se compose de deux personnes représentant les Services financiers, deux personnes représentant les Services des technologies de l'information.

**PR1.2.**

La personne-ressource pour tous les commerçants est la superviseure ou le superviseur des Services bancaires des Services financiers.

## PR2. Responsabilité administrative

**PR2.1.**

Les Services financiers et les Services des technologies de l'information se partagent la responsabilité de la conformité aux normes PCI et de l'attestation de conformité de l'Université.

**PR2.2.**

Responsabilités du Comité directeur sur la conformité aux normes PCI :

a) Interprétation et communication des lignes directrices de conformité aux normes PCI
b) Approbation des fournisseurs de traitement des paiements, des fournisseurs de lecteurs et des évaluatrices et évaluateurs de sécurité qualifiés.
c) Approbation des commerçants.
d) Remise aux commerçants du questionnaire d'autoévaluation annuelle de la conformité à la norme PCI DSS approprié selon leur type d'activités.
e) Approbation des réponses justifiées des commerçants au questionnaire d'autoévaluation annuelle de la conformité à la norme PCI DSS.
f) Retrait à un commerçant du droit de traiter les paiements par carte.

**PR2.3.**

La responsabilité de l'approbation des demandes motivées des commerçants et des obligations fiscales relève des Services financiers. Ces éléments font l'objet d'un examen annuel.

**PR2.4.**

La responsabilité de l'architecture et du déploiement de solutions relève des Services des technologies de l'information, y compris le développement ou l'acquisition de logiciels destinés à l'usage des commerçants.

**PR2.5.**

La responsabilité de la passerelle de paiement électronique de McGill relève des Services des technologies de l'information.

**PR2.6.**

La responsabilité de présenter des réponses justifiées au questionnaire d'autoévaluation annuelle de la conformité à la norme PCI DSS relève de chaque commerçant. La ou le responsable de l'unité doit approuver les réponses.

**PR2.7.**

La responsabilité des contrôles et des mesures d'atténuation des risques relève de chaque commerçant, à ses propres frais.

**PR2.8.**

La responsabilité de la confirmation annuelle des renseignements de la demande motivée relève de chaque commerçant.

**PR2.9.**

La responsabilité de répondre au questionnaire d'autoévaluation annuelle de la conformité à la norme PCI DSS au nom de l'Université relève des Services financiers et des Services des technologies de l'information. Ce questionnaire doit être soumis à l'approbation du Comité directeur sur la conformité aux normes PCI.

**PR2.10.**

La responsabilité de s'assurer que le respect des normes PCI est énoncé dans les conditions des contrats, s'il y a lieu, relève du Service des approvisionnements.

**PR2.11.**

La responsabilité de la destruction des documents relève des Archives de l'Université McGill et de l'unité ou de la personne responsable de la conservation des données en lieu sûr. Les renseignements des cartes de paiement doivent être conservés séparément des autres renseignements pour faciliter le respect des exigences de sécurité, de conservation et d'élimination des données.

## PR3. Création de comptes marchands

**PR3.1.**

Les commerçants doivent envoyés le Questionnaire à l'intention des commerçants dûment rempli à l'attention de la superviseure ou du superviseur des Services bancaires des Services financiers.

**PR3.2.**

Les Services financiers étudient le questionnaire à l'intention des commerçants (y compris les obligations fiscales).

**PR3.3.**

Les Services financiers envoient au commerçant un questionnaire d'évaluation à remplir et à envoyer au Comité directeur sur la conformité aux normes PCI, qui déterminera le questionnaire d'autoévaluation annuelle de la conformité à la norme PCI DSS approprié pour le type de commerçant.

**PR3.4.**

En collaboration avec les fournisseurs de traitement des paiements, les Services financiers envoient au nouveau commerçant l'approbation écrite et les instructions nécessaires.

**PR3.5.**

Les unités doivent respecter la Politique sur les transactions financières par flux de données, qui régit le transfert de données dans le Système d'information des Services financiers (SISF).

## PR4. Définitions

**PR4.1. Code de vérification de la carte (CVC)**
Code à trois chiffres imprimé au verso de la carte de crédit à droite de la signature, à la suite du numéro de la carte. Sur les cartes American Express, ce code se compose de quatre chiffres et est imprimé au recto de la carte, au-dessus du numéro. Ce code est associé à la carte elle-même et la relie au numéro de compte de crédit.

**PR4.2. Données des titulaires de carte**
Renseignements liés à une carte de crédit, de débit ou prépayée, soit le numéro de la carte et possiblement le nom de la ou du titulaire, la date d'expiration, le code de vérification de la carte ou le code de service.

**PR4.3. Réponses justifiées**
Les commerçants doivent fournir des justifications à leurs réponses (par oui ou non) dans le questionnaire d'autoévaluation de la conformité à la norme PCI DSS, afin de faciliter l'évaluation par le Comité directeur sur la conformité aux normes PCI et le processus annuel de renouvellement de l'attestation.

**PR4.4. Commerçant**
Toute unité autorisée par l'Université (Services financiers) à accepter des paiements par carte de crédit, de débit ou prépayée pour l'achat de biens ou de services ou le versement de dons.

**PR4.5. Centre de ressources des commerçants**
Portail pour les commerçants en ligne offrant des fonctions de production de rapports et d'administration, ainsi qu'un terminal virtuel pour le traitement des remboursements ou annulations.

**PR4.6. PCI Standard Logicielle Sécurisée (SSF)**
Norme de sécurité des données des applications de paiement régissant le développement d'applications de paiement sécurisées qui ne stockent pas illégalement de données comme la bande magnétique ou le code de vérification de la carte.

**PR4.7. Conseil des normes de sécurité du secteur des cartes de paiement (PCI SSC)**
Organisme de normalisation qui définit les normes du secteur des cartes de paiement.

**PR4.8. Fournisseur de traitement des paiements**
Fournisseur qui gère le traitement et le règlement des transactions par carte de crédit, de débit ou prépayée pour les commerçants de l'Université.

**PR4.9. PCI**

Sigle désignant le secteur des cartes de paiement, qui forme un conseil de sécurité fondé par les cinq grands fournisseurs de cartes de crédit (American Express, Visa Inc., MasterCard Worldwide, Discover Financial Services et JCB International).

**PR4.10. PCI-DSS**

Norme de sécurité des données du secteur des cartes de paiement.

**PR4.11. Conservation en lieu sûr**

Les documents contenant des données de titulaires de carte doivent être conservés en lieu sûr, c'est-à-dire dans un endroit sous clé dont l'accès est réservé au personnel autorisé.

## PR5. Documents connexes

**PR5.1.**

Politique sur l'utilisation responsable des ressources en technologie de l'information de l'université McGill

**PR5.2.**

Norme PCI SSC

**PR5.3.**

Bibliothèque de document du PCI SSC

**PR5.5.**

PCI Standard Logicielle Sécurisée (SSF)

**PR5.6.**

Guide à l'intention des commerçants de McGill pour le traitement de paiements par carte de crédit (en anglais)

**PR5.7.**

Grille d'évaluation des taxes de vente pour les congrès nationaux (en anglais)