UNIVERSITÉ DE SHERBROOKE

DIRECTIVE 2600-084

TITRE :	**Directive relative à la sécurité de la perception par carte de crédit**		
ADOPTION :	Comité de direction de l'Université	Résolution :	CD-2020-09-14-06
ENTRÉE EN VIGUEUR :	14 septembre 2020		

TABLE DES MATIÈRES

1. PRÉAMBULE

La norme PCI DSS (Payment Card Industry Data Security Standard) est un ensemble complet d'exigences auxquelles les entreprises qui traitent les paiements par cartes de crédit ou de débit doivent répondre, quels que soient l'importance et le nombre de transactions traitées afin d'utiliser de façon sécuritaire ce mode de paiement.

L'Université de Sherbrooke souhaite se conformer à ladite norme afin d'assurer la protection des données de paiement confidentielles. Ces données soutiennent les objectifs d'affaires de l'Université.

2. OBJECTIF

L'objectif de cette directive est d'énoncer les exigences applicables à tous les secteurs de l'Université qui stockent, traitent ou transmettent des données de détenteurs de carte de crédit et d'établir les responsabilités de tous les intervenants impliqués dans le processus afin de réduire le risque entourant l'utilisation desdites données et d'améliorer les processus de perception par carte de crédit à l'Université.

Cette directive ne remplace aucune disposition de toute autre politique universitaire pertinente et doit être appliquée conjointement avec la *Directive relative à l'utilisation, à la gestion et à la sécurité des actifs informationnels* (Directive 2600-063) et la *Politique de sécurité de l'information* (Politique 2500-036).

3. CHAMP D'APPLICATION

Cette directive s'applique à tous les membres du personnel autorisés, au personnel de La Fondation de l'Université et aux sous-traitants de l'Université qui, dans le cadre de leurs fonctions, utilisent des mécanismes de perception par carte de crédit ou ont accès aux systèmes de cartes de crédit ou aux données des détenteurs de cartes de crédit. Elle s'applique également à toute entité ou toute personne ayant l'intention d'utiliser les transactions par carte de crédit au nom de l'Université.

Cette directive vise l'ensemble des transactions liées à la perception par carte de crédit.

4. RESPONSABILITÉS

4.1 Les responsabilités du Service des ressources financières

Il incombe au Service des ressources financières (SRF) de sécuriser les systèmes de cartes de crédit ainsi que les données des titulaires de cartes de crédit <u>sur tous les supports</u>, en :

- S'assurant de l'application de cette directive;
- Veillant à ce que cette directive soit révisée régulièrement et que des modifications soient recommandées au besoin;
- Autorisant au préalable les mécanismes de perception par carte de crédit utilisés par l'Université;
- S'assurant qu'une attestation de conformité PCI DSS valide ait été obtenue pour tous les fournisseurs de paiement utilisés par l'Université avant d'accorder une autorisation d'installation d'un mécanisme de perception par carte de crédit;
- Assurant une vigie de l'utilisation des mécanismes de perception par carte de crédit dans les différentes unités administratives;

- Étant l'unité responsable des modalités de perception par carte de crédit à l'Université avec la collaboration du Service des technologies de l'information pour les composantes techniques;

- Formant le personnel autorisé à accéder au système et aux données des détenteurs de cartes de crédit sur les meilleures pratiques concernant la sécurité des transactions par carte de crédit;

- Produisant et en maintenant un inventaire à jour de tous les mécanismes de perception par carte de crédit à l'Université;

- Obtenant les mises à jour des attestations de conformité PCI DSS pour tous les fournisseurs de paiement utilisés par l'Université.

4.2 Les responsabilités du Service des technologies de l'information

Il incombe au Service des technologies de l'information (STI) de sécuriser les systèmes de paiement par carte de crédit ainsi que les données des titulaires de cartes de crédit sur tous les supports numériques, en:

- Servant d'appui au Service des ressources financières pour toute composante technique entourant l'utilisation d'un mécanisme de perception par carte de crédit à l'Université;

- Prenant les mesures techniques appropriées pour s'assurer que les données sensibles des titulaires de cartes de crédit ne sont pas stockées sur le système informatique de l'Université;

- Architecturant de manière efficace et sécuritaire les systèmes traitant les données sensibles des titulaires de cartes de crédit;

- Contrôlant l'utilisation sécuritaire des ressources mises en place pour le traitement des données sensibles des titulaires de cartes de crédit;

- Conseillant toutes les entités de l'Université sur le traitement desdites données.

4.3 Les responsabilités du personnel autorisé à accéder au système et aux données des détenteurs de carte de crédit

Il incombe aux utilisateurs autorisés de sécuriser les systèmes de cartes de crédit et les données des titulaires de carte de crédit sur tous les supports numériques, en :

- Obtenant une autorisation préalable du Service des ressources financières pour l'installation d'un mécanisme de perception par carte de crédit;

- S'abstenant de stocker de l'information relative aux cartes de crédit sous quelque forme que ce soit;

- Répondant annuellement au questionnaire d'auto-évaluation et en signant l'attestation de conformité;

- Traitant avec des fournisseurs de paiement détenant une attestation de conformité PCI DSS valide;

- Caviardant les numéros des cartes de crédit des formulaires conservés;

- Entreposant les formulaires caviardés dans un endroit sécuritaire et verrouillé;

- Détruisant de façon sécuritaire tout document qui contient des informations de détenteurs de carte de crédit;

- Refusant de recevoir par courriel toute information relative aux cartes de crédit;

- Informant toute personne effectuant une transaction par carte de crédit non sécuritaire des bonnes pratiques, le cas échéant.

4.4 Les responsabilités du comité de suivi à la conformité PCI DSS

Un comité de suivi à la conformité PCI DSS est formé et le mandat suivant lui est attribué :

- Identifier des pistes d'amélioration à la conformité PCI DSS;

- Maintenir les risques liés à la sécurité des informations de paiement à un niveau acceptable;

- Suivre le plan d'amélioration annuel proposé par le Service des ressources financières et par le Service des technologies de l'information pour la portion technique.

Le comité est présidé par la directrice ou le directeur de la section comptabilité du Service des ressources financières et formé d'une représentante ou un représentant des unités administratives suivantes :

- Bureau de la registraire;

- Centre culturel;

- La Fondation de l'Université de Sherbrooke;

- Secrétariat général;

- Service des technologies de l'information;

- Vice-rectorat à la recherche et aux études supérieures.

Le comité se réunit au moins une fois par année.

5. RESPONSABILITÉ DE LA DIRECTIVE

Le membre du comité de direction de l'Université duquel relève le Service des ressources financières est responsable de l'application, de la mise à jour et de la diffusion de la présente directive.

6. ENTRÉE EN VIGUEUR

La présente directive entre en vigueur le 14 septembre 2020.