POLITIQUE – SÉCURITÉ DES CARTES DE CRÉDIT

Date d'entrée en vigueur : 1er mai 2014

Origine : Cabinet du chef de la direction financière

Version remplacée ou amendée : S. O.

Numéro de référence : CFO-9

PRÉAMBULE

La présente politique traite des exigences de l'Université Concordia (« l'Université ») en matière de sécurité des cartes de crédit. Elle s'inspire de la *Norme de sécurité des données* établie par l'Industrie des cartes de paiement (« l'ICP »). L'Université entend ainsi assurer la protection de l'information qu'elle utilise pour réaliser ses objectifs d'affaires.

OBJET

La présente politique a pour but d'appliquer les normes de l'ICP à l'ensemble des systèmes qui, à l'Université, servent au stockage, au traitement ou à la transmission de données sur les titulaires de carte de crédit. L'utilisation par l'Université de cartes de crédit est limitée à des applications de paiement reliées à Internet. En règle générale, elle n'englobe pas le stockage de données relatives aux titulaires de carte de crédit, et ce, sur quelque système informatique que ce soit.

La présente politique n'annule aucune disposition contenue dans toute autre politique pertinente de l'Université. De plus, elle doit être lue en parallèle avec le *Code des droits et des obligations* (BD-3), la politique *Protection des renseignements personnels* (SG-9) et la politique *Installations informatiques* (VPSS-30).

PORTÉE

La présente politique concerne toute personne habilitée – qu'elle soit membre permanent du corps professoral ou du personnel de l'Université, ou encore entrepreneur externe – bénéficiant dans le cadre de ses fonctions d'un accès à des systèmes de cartes de crédit ou à des données sur des titulaires de carte de crédit, et ce, peu importe le support utilisé (« les utilisateurs autorisés »), de même qu'à toute autre entité ou personne qui compte effectuer des opérations par carte de crédit au nom de l'Université.

POLITIQUE

1. Le chef de la direction financière de l'Université est responsable de l'application de la présente politique.

2. Il incombe au chef de la direction financière de l'Université de s'assurer que la présente politique – y compris toute consigne, procédure ou norme associée – soit revue au moins une fois par année. S'il y a lieu, il recommande alors que des amendements y soient apportés.

3. À l'Université, nul ne peut installer un système de cartes de crédit sans avoir obtenu l'autorisation préalable des Services financiers.

4. Il incombe aux Services financiers de sécuriser les systèmes de cartes de crédit et les données sur les titulaires de carte de crédit, et ce, peu importe le support utilisé. À cette fin, les Services financiers :

   - autorisent et facilitent l'installation du matériel nécessaire à l'exécution d'opérations par carte de crédit. Par ailleurs, conformément à la politique *Gestion des immobilisations* (CFO-4) de l'Université, ils tiennent à jour l'inventaire dudit matériel;

   - collaborent avec les unités intéressées afin de limiter aux seuls utilisateurs autorisés l'accès aux systèmes de cartes de crédit de l'Université et aux données sur les titulaires de carte de crédit. Ils dressent également une liste centralisée des utilisateurs autorisés;

   - adoptent s'il y a lieu des mesures et établissent au besoin des directives à l'intention des utilisateurs autorisés afin d'encadrer la conservation sécuritaire des données sur les titulaires de carte de crédit ainsi que leur destruction en toute sûreté lorsqu'elles ne sont plus utiles;

   - mettent en œuvre des mesures pour que seuls les entrepreneurs externes agréés par l'ICP puissent être considérés comme des utilisateurs autorisés. À cet égard, avant d'accorder à ces derniers l'accès à tout système de cartes de crédit ou à toute information sur les titulaires de carte de crédit, les Services financiers s'assurent que les documents juridiques pertinents sont établis à la satisfaction de l'Université;

   - retirent – après avoir consulté les unités intéressées – le titre d'utilisateur autorisé à toute personne qui n'a plus besoin d'accéder, dans le cadre de ses fonctions, aux systèmes de cartes de crédit ou aux données sur les titulaires de carte de crédit;

- avisent les utilisateurs autorisés qu'il leur incombe de recenser tout incident lié à la sécurité technologique, et ce, afin de faciliter la mise en œuvre du plan d'intervention et des procédures en la matière;
- coopèrent avec les unités intéressées afin de relayer l'information relative à tout incident lié à la sécurité technologique (« incident de TI ») aux parties concernées – émetteurs de cartes de crédit, fournisseurs de services et, s'il y a lieu, autorités locales.

5. Il incombe au Service des technologies de l'information et de l'enseignement de l'Université de sécuriser les systèmes de cartes de crédit et les données sur les titulaires de carte de crédit, et ce, peu importe le support utilisé. À cette fin, le service :

- gère un réseau sécurisé;
- change les mots de passe par défaut des systèmes intégrés à tout équipement de réseautique et recourt à des techniques de cryptage éprouvées aux fins de l'authentification et de la transmission des données;
- supprime tout service ou protocole superflu des systèmes de cartes de crédit;
- fournit un accès crypté aux systèmes administratifs à interface réseau (« non console »);
- met en œuvre les moyens techniques appropriés pour que les données sensibles sur les titulaires de carte de crédit ne soient stockées qu'en cas de nécessité absolue;
- veille à l'installation de logiciels antivirus sur tout système de l'Université servant à l'exécution d'opérations par carte de crédit et s'occupe de leur actualisation;
- s'assure de la mise en place de correctifs critiques sur tout système de l'Université servant à l'exécution d'opérations par carte de crédit;
- adopte des mesures visant à restreindre l'accès physique à tout système de cartes de crédit ou support de l'Université hébergeant des données sur les titulaires de carte de crédit;
- vérifie régulièrement les systèmes et processus de sécurité;
- veille à ce que tout utilisateur autorisé obtienne son propre code d'identification;

- mappe et surveille l'activité des utilisateurs autorisés ainsi que de tout dispositif dont ils se servent;
- adopte des mesures de déconnexion automatique de toute séance effectuée au moyen des télétechnologies;
- élabore, documente et diffuse des procédures d'intervention et de recours à la hiérarchie en cas d'incident de TI, et ce, afin d'assurer la gestion efficace et rapide de tout incident en matière de sécurité technologique;
- déclare tout incident de TI conformément aux procédures établies par les Services financiers.

6. Il incombe aux utilisateurs autorisés de sécuriser les systèmes de cartes de crédit et les données sur les titulaires de carte de crédit, et ce, peu importe le support utilisé. À cette fin, ils :

- se conforment aux dispositions de la présente politique, de même qu'aux mesures et directives prescrites par les Services financiers;
- collaborent aux procédures d'intervention faisant suite à tout incident technologique dans leur sphère de responsabilité.