POLICY NAME	MERCHANT (PCI) POLICY & PROCEDURES - ACCEPTING CREDIT/DEBIT CARD PAYMENTS
Revision	V1.7
Publication Date	August 11, 2009
Revision Date	November 12, 2024
Effective Date	November 12, 2024

PURPOSE AND SCOPE

There are many units across campus that store, process or transmit cardholder data for credit and debit card payments to the University for goods and services provided as well as for donations. Credit/debit/pre-paid card payments must comply with standards set forth by the Payment Card Industry Data Security Standards, otherwise known as PCI-DSS. The goal of PCI-DSS is to protect cardholder data including any processes, systems and transmissions relating to credit/debit/pre-paid card payments.

University systems and processes must be certified as 'PCI compliant' to process credit/debit/pre-paid card payments. Certification is attained at an institutional level, and therefore all merchants at McGill must ensure their business practices conform to the standards outlined in this policy. Non-compliance exposes the University to:

- Higher potential of fraudulent charges to the cardholders;
- Poor service to students, alumni and general public;
- Fines;
- Impact on the University's reputation;
- Loss of certification, resulting in the University's inability to accept and process any future credit/debit/pre-paid card payments.

Refer to the Procedures for details regarding the implementation and interpretation of the following policies.

SCOPE

This policy applies to all University employees who are involved in accepting or processing credit/debit/pre-paid card payments for McGill and those involved in providing infrastructure to support such services. It is the responsibility of employees to ensure that other involved parties (e.g. students, volunteers, third party vendors) comply with this Policy. Entities who are at arm's length from McGill but use McGill's name must comply with this Policy. Non-compliance could result in McGill's name, reputation and certification being compromised. For the purposes of this Policy, "employee" collectively refers to academics, researchers, and administrative staff.

Only units recognized and accepted by the University (Financial Services) are deemed as "merchants" and can proceed to process credit/debit/pre-paid card payments. All merchants, regardless of processing method, must comply with this policy.

E-Commerce merchants
The cardholder makes an online purchase or donation, and is prompted to enter their credit card number, expiration date and card verification code or value.

Point of sale (POS) merchants
The point of sale 'store' uses a terminal from the University's contracted payment processing vendors. The cardholder is physically present when making the purchase and their card is swiped or entered through the point of sale terminal. The payment is considered processed when receipt of an authorization code is sent to the merchant.

IVR merchants (interactive voice response)
Without an internet solution or a physical terminal, the IVR merchant enters the credit card information (number, expiry date) via the University's contracted vendor payment processing automated phone system to gain an authorization code. If the cardholder is present, the merchant will use the imprint as proof of payment.

POLICY

P1.

All University merchants must abide by this policy. Failure to abide with this Policy to the satisfaction of the PCI Compliance Steering Committee will result in the revocation of the merchant's capabilities.

P2. Merchant Accounts

Any unit setting up an operation to receive payments (for goods or services rendered or to receive donations) must be given an approved University merchant account. Financial Services is the **only** administrative body entitled to create merchants, hence, all internet, point of sale, and interactive voice response merchants must be **pre-approved** in writing by Financial Services to ensure that:

- All credit/debit/pre-paid card transactions are processed via the University's contracted payment processing vendor(s); and
- All revenues will be deposited in a central University bank account approved by Financial Services.

P3. Bank Accounts

A McGill unit cannot open a bank account or any type of account (e.g. Paypal) to receive payments in the name of the University. Financial Services is the sole authorized unit to establish bank accounts to receive payments in the name of the University.

P4. Payment Card Industry Data Security Standard (PCI DSS)

The Payment Card Industry Security Standards Council (PCI SSC) sets the Payment Card Industry Data Security Standards (PCI DSS), which are enforced by card brands. PCI SSC and card brands see McGill University as a single entity, with a single PCI chain. This means that non-compliance of PCI DSS for one McGill University merchant account could affect all McGill University merchant accounts.

All credit/debit/pre-paid card transactions must comply with Payment Card Industry Data Security Standard (PCI DSS) to ensure that the University maintains its capability to process such payments. Any requirements defined by the PCI Compliance Steering Committee must be met.

P5. Confidentiality of Cardholder Data

Cardholder data can neither be stored electronically (e.g. spreadsheet, network drive, database server) nor transmitted/received by electronic messaging (e.g. email, instant messaging) nor VoIP (Voice over IP).

P6. Supporting Documentation, Records Retention and Disposition

All financial transactions must be substantiated with supporting documentation. For payments received, examples include a receipt or invoice to support for what, why and by whom the payment was made. Supporting documentation must be retained according to the University's Retention rules (MURRS), typically seven years.

Proof of settlement (credit card chit or imprint) is not required to substantiate the financial transaction, since evidence exists on the University's bank account. Proof of settlement that includes cardholder data must be stored securely (lock and key, restricted on a business need-to-know basis) for a period of 18 months for the sole purpose of responding to disputes. Proof of settlement must be destroyed immediately after this time.

Merchants must design their documentation templates such that cardholder information does not appear on records that are accessible by many or require long-term retention. Any historical documents considered supporting documentation which include proof of settlement (and thereby sensitive cardholder information) must be limited to paper and securely stored with restricted access. Exceptionally, with prior written approval of the PCI Compliance Steering Committee, cardholder data may be scanned in authorized digital repositories.

P7. Services and Solutions

Solutions or services that use a McGill University merchant account, solutions or services using supplier merchant accounts, services of an alternate acquirer or payment service provider, concession services are in-scope of this policy. Any McGill developed software and any third-party services or solutions that access, store, process or transmit credit card information, or could impact on the security of cardholder data, must be assessed and approved by the PCI Compliance Steering Committee as McGill is contractually obliged to get an approval from our contracted acquirer.

PCI compliance must be incorporated into any contracting process for contracts that

deal with PCI aspects as defined by this policy.

P8. Incident Reporting

Any security incident relating to cardholder data must be reported immediately to the Banking Supervisor, Financial Services.

Financial Services will advise Information Technology Services in accordance with established protocols.

P9. Change Management

Any business process, system, infrastructure or application change that would alter one's answers to the PCI Compliance Steering Committee (e.g. Merchant Questionnaire, the PCI DSS Self-Assessment Questionnaire) requires immediate reporting to the Banking Supervisor, Financial Services.

PROCEDURES

PR1. PCI Compliance Steering Committee

PR1.1.

PCI Compliance Steering Committee will be guided by PCI Compliance best practices and risk assessments. McGill's PCI Compliance Steering Committee consists of two delegates from Financial Services, two delegates from Information Technology Services.

PR1.2.

The key contact for all merchants is the Banking Services Supervisor in Financial Services.

PR2. Administrative Responsibility

PR2.1.

Responsibility for PCI Compliance including the University's certification resides jointly with Financial Services and Information Technology Services.

PR2.2.

The PCI Compliance Steering Committee is:

a) Responsible for McGill's interpretation and communication of PCI Compliance guidelines.
b) Responsible for approving payment processing vendors, scanning vendors and also qualified security assessors.
c) Responsible for approving merchants.
d) Responsible for providing the corresponding PCI DSS Annual Self-Assessment Questionnaire to the merchant depending on their type of operation.
e) Responsible for reviewing and accepting the merchant's fully annotated response to the PCI DSS Annual Self-Assessment Questionnaire.
f) Responsible for the revocation of a merchant's capabilities.

PR2.3.

Responsibility for the review and approval of the business case and tax implications for all merchants resides with Financial Services. This will also be reviewed on an annual basis.

PR2.4.

Responsibility for the architecture and implementation resides with Information Technology Services, including the development or the purchase of software to be used by merchants.

PR2.5.

Responsibility for the McGill E-payment gateway resides with Information Technology Services.

PR2.6.

Responsibility for preparing a fully annotated response to the PCI DSS Annual Self-Assessment Questionnaire resides with each merchant and is signed by the unit head.

PR2.7.

Responsibility for implementing controls and processes to mitigate risk resides with each merchant at their cost.

PR2.8.

Responsibility for confirming, on an annual basis, the business case resides with each merchant.

PR2.9.

Responsibility for responding to the PCI DSS Annual Self-Assessment Questionnaire on behalf of the entire University resides with Financial Services and Information Technology Services. The Questionnaire will be submitted to and reviewed by the PCI Compliance Steering Committee.

PR2.10.

Responsibility to ensure that University contractual agreements, where applicable, stipulate adherence to PCI Compliance resides with Procurement Services.

PR2.11.

Responsibility for document destruction lies with McGill University Archives and with the unit or person responsible for the secure retention of the data. Cardholder information should be kept separately from the rest of the information as to ease and assist in compliance with the security, retention and disposition requirements.

PR3. Creation of Merchants

PR3.1.

Complete the "Merchant Questionnaire" and send it to the attention of the Banking Services Supervisor, Financial Services to banking@mcgill.ca.

PR3.2.

Financial Services will review the Merchant Questionnaire (including tax implications).

PR3.3.

Financial Services will send the merchant a survey to be completed. The completed survey will be forwarded to the PCI Compliance Steering Committee and will be used to determine the appropriate PCI DSS Annual Self-Assessment Questionnaire to be completed by the merchant.

PR3.4.

Financial Services will coordinate and provide written approval and instructions to the new merchant with the University contracted payment processing vendors.

PR3.5.

Units must comply with the Financial Transactions Feed Policy, which governs how data is transferred into our Financial Information System (FIS).

PR4. Glossary of Terms

PR4.1. Card Verification Code or Value

Three-digit value printed to the right of the credit card number in the signature panel area on the back of the card. For American Express cards, the code is a four-digit unembossed number printed above the card number on the face of all payment cards. The code is uniquely associated with each individual piece of plastic and ties the card account number to the plastic.

PR4.2. Cardholder Data

Credit/debit/pre-paid card information, including the primary account number possibly with any of the following: cardholder name, expiration date, card verification value or service code.

PR4.3. Fully Annotated Questionnaire

Merchant responses (yes/no answers) to the PCI DSS Self-Assessment Questionnaire need to be qualified (annotated) with supporting justifications. This process not only allows the PCI Compliance Steering Committee to evaluate responses but also simplifies the annual recertification process.

PR4.4. Merchant

Any McGill unit that accepts credit/debit/pre-paid cards as payment for goods, services and/or services or donations, and who has been authorized to do so by the University (Financial Services).

PR4.5. Merchant Resource Centre

Web-based tool for e-commerce merchants which offers reporting, administrative functions as well as virtual terminal which is used for processing refunds or voids.

PR4.6. PCI Software Security Framework (SSF)

Payment Application Data Security Standards: to help software vendors and others develop secure payment applications that do not store prohibited data, such as full magnetic stripe or card verification code or value.

PR4.7. Payment Card Industry Security Standards Council (PCI SSC)

PCI SSC is the standards body that maintains the payment card industry standards.

PR4.8. Payment Processing Vendor(s)

Provide credit/debit/pre-paid card transaction processing and settlement to the University's merchants.

PR4.9. PCI

Payment Card Industry, a security council founded by the five major credit card providers (American Express, Visa Inc., MasterCard Worldwide, Discover Financial Services and JCB International).

PR4.10. PCI-DSS

Payment Card Industry Data Security Standards.

PR4.11. Secured Storage

Any documentation containing cardholder data must be securely stored. That is to say, using a safe or lock/key, with restricted access on a business need-to-know basis.

PR5. Links to Related Documents

PR5.1.

IT Policies

PR5.2.

PCI Standards Overview

PR5.3.

PCI DSS Document Library

PR5.4.

PCI Software Security Framework

PR5.5.

Merchant Tool kit

PR5.6.

Sales Tax Assessment Matrix on Domestic Conventions