McMaster University

Administration Policy

Complete Policy Title: **Policy for Acceptance of Payment Cards and eCommerce Payments**	Policy Number:
Approved by: **Vice-President (Administration)**	Date of Most Recent Approval: **March 2021**
Date of Original Approval: **August 2005**	Supersedes/Amends Policy dated: **November 2011**
Responsible Executive: • **Assistant Vice-President (Administration) & CFO** • **Assistant Vice President & Chief Technology Officer**	Enquiries: **finserv@mcmaster.ca** **c-it-security@mcmaster.ca**
DISCLAIMER: *If there is a discrepancy between this electronic policy and the written copy held by the policy owner, the written copy prevails.*	

A. Purpose

1. The Payment Card Industry ["PCI"] has established industry standards for the processing of purchase transactions electronically.
2. It is critical that the process for accepting, processing and storage of information relating to Card transactions be secure to (i) protect privacy and personal information and (ii) safeguard Card users' bank accounts and other assets.
3. All Merchants/Departments/Faculties ["Departments"] must meet the University's requirements for payment security and for integrating transaction information in to the University's systems.

B. Scope

1. This Policy is applicable to all Departments and affiliates wishing to process Payment Card and eCommerce transactions using any of the following:
    - website [eCommerce],
    - entered by staff from information provided by the customer
    - point of sale ["POS"] terminals,
    - third-party hosted services.
2. Separate legal entities processing Payment Card and eCommerce transactions on behalf of McMaster, or whose systems reside on the McMaster network, must attest they meet PCI requirements as outlined in this Policy.

C. Definitions

Payment Card – Payment cards are part of a payment system that enables cardholders to make a payment by electronic funds transfer. The most common types of payment cards are credit cards and debit cards. Refer to the Financial Affairs website for accepted cards.

PCI-DSS – The Payment Card Industry Data Security Standard (PCI DSS) is a set of security standards designed to ensure that ALL companies that accept, process, store or transmit credit card information maintain a secure environment. (pcicomplianceguide.org)

Preferred Payment Provider – The University has a contractual relationship with a primary payment processor who provides preferential payment card processing rates, and shares responsibility for mitigating payment card risk.

Approved Alternate Payment Provider(s) – Other payment processors reviewed by McMaster Financial Affairs and UTS Information Security Services for use when the Preferred Payment Provider does not meet the departments' needs. McMaster Financial Affairs maintains the list of Payment Providers who have been approved by PCI DSS Steering Committee.

Daily – for the purpose of this Policy, daily refers to next McMaster business day.

D. Policy

1. Department Responsibilities

a. The processing of Card transactions must be done by a University approved payment provider.

b. Departments must adhere to the most recent version of the Payment Card Industry Data Security Standard (PCI-DSS) at all times.

c. Departments may not enter into separate banking and/or payment processing arrangements.

d. Departments are responsible for retaining transaction records for audit purposes for seven years.

e. The University Statement on Collection of Personal Information and Protection of Privacy applies to payment card transactions.

f. All Department staff receiving or handling payments must be familiar with the contents of the University's Fraud Policy and conduct their affairs accordingly.

g. Departments are responsible for all fees both internal and external. External fees are those charged by the payment processor and card brands. Internal fees are those charged by Financial Affairs and University Technology Services to cover the costs associated with managing the Payment Card and eCommerce program at the university.

Service	**Fee**	**Notes**
Virtual Terminal or eCommerce merchant	$750* per year and 1.25% on sales	Maximum % fee of 12,000
POS or Alternative Payment Provider Merchant	$350* per year and 1.25% on sales	As above
Small Volume Transaction Processing (SVTP)	$10 per month and 1.25% on sales	Up to 10 transactions per month, else dept. must become own merchant

*If merchant account is not in use, departments must advise Financial Affairs, to avoid this charge.

2. Payment Providers

a. The University has a Preferred Payment Provider. Departments must use the Preferred Payment Provider unless it is technically unfeasible. McMaster Financial Affairs and Information Security Services will review departments' application to use an Approved Alternate Payment Provider.

b. If a department finds that they are unable to use the Preferred Payment Provider or one of the Approved Alternate Payment Providers, application may be made to the PCI DSS Steering Committee's attention to review additional payment processors/providers. It is recommended that the Department work with McMaster Financial Affairs and Information Security Services to clarify the need and suitability before making application to the Committee. Upon receiving PCI committee's approval the department will work with McMaster Financial Affairs and Information Security Services to implement the change.

c. Payment Providers are used to collect payments and transfer funds to McMaster. All funds received must be deposited into a McMaster bank account as directed by McMaster Financial Affairs. In the event that a refund of a payment received from a Payment Provider must be made, refer to the procedures document. Payment Providers must not be used for any outgoing payments other than refunds of previously received payments.

d. Deposits must be performed daily to a McMaster bank account directed by McMaster Financial Affairs. Reconciliations and Mosaic deposits must be done daily, or each day for which there are transactions.

e. Payment Providers cannot be used for general fundraising or Advancement purposes without the oversight of McMaster Advancement Services.

f. All Payment Provider accounts will have at least the following four University employees with the ability to review transactions,
   - Department Signing Authority
   - Finance person in the owner department
   - Representative from McMaster Student Accounts and Cashiers
   - McMaster's Manager of Financial Reporting

   If the Department Signing authority is the same person as the financial manager, another department representative should be attached to the account to ensure segregation of duties and appropriate oversight.

g. Every person that is required to login to the Payment Processor must do so using credentials which are only used by them (i.e., unique), and can clearly be identified as their credentials (i.e., identifiable). If the Payment Processor does not allow sufficient login IDs for every person that is required to login, the department will work with Information Security Services to develop an appropriate access protocol.

h. Personal email accounts (e.g., non McMaster) must not be used for communication with Payment Providers.

3. Technology Standard

a. Merchants are responsible for ensuring that their payment solutions, and the systems on which they run, comply with all relevant Payment Card Industry Data Security Standard (PCI-DSS) requirements. PCI-DSS requirements are grouped into six parts:

1) Build and Maintain a Secure Network and Systems
2) Protect Cardholder Data
3) Maintain a Vulnerability Management Program
4) Implement Strong Access Control Measures
5) Regularly Monitor and Test Networks
6) Maintain an Information Security Policy

b. All eCommerce merchants must have additional security controls to prevent fraudulent attacks against their hosted pay page.

1) Merchants must implement "Data Preload" control. Merchant should ensure that all code and variables that support Data Preload are kept secure at all times
2) Merchants must enable session logging to track attributes of the customer eCommerce transaction requests. Specifically, the customer "session ID" and the customer "IP address" must be tracked. This information will be necessary to support investigations of fraudulent activity.
3) Merchants must implement CVV and AVS security controls.

c. Merchants must not implement eCommerce solutions through which cardholder data is processed by the merchant. All cardholder data must be processed only by the payment provider.

d. Merchants must not store cardholder data in electronic format.

e. Merchants must not use e-mail to initiate and/or effect a transaction. Merchants must not send cardholder data via email.

f. Payment solutions, and the systems on which they run, must be audited by Information Security Services before implementation. Merchants that reuse existing merchant numbers to receive payments using another solution must inform Information Security Services, and are subject to another audit. Merchants are subject to external security audits, at the expense of the department.

g. Merchants are responsible for maintenance of their payment solutions, and the systems on which they run, including all software upgrades and patches to known vulnerabilities. Payment solutions will be assessed for vulnerabilities periodically by Information Security Services. Payment solutions must be assessed any time there is a change to a system.

4. Compliance

a. Each Department Account Signing Authority, or delegate, must attend the University's training sessions and attest to compliance with this policy when notified by PCI DSS Steering Committee that such attestation is due.

b. Existing Departments which change their process and/or software integrated with the payment functionality are required to complete [re]-approval documentation for their system in accordance with this Policy.

c. Departments found to have inadequate security may have their merchant number suspended.

d. The suspension process of the merchant number account may include:

Notification of the results of vulnerability scan and/or Internal Audit notification of a breach of PCI requirements and/or lack of adherence to this Policy. Such notification will ask that remedial action be taken and for the Department to report back on the action(s) taken.

If remedial actions are incomplete and/or undue time elapses without resolution, a final request for compliance will be sent with expectation that the Department will provide a written plan indicating who is resolving the issues and by when.

e. Depending on the severity of non-compliance, the account may be suspended immediately and not restored until the Department has completed all applicable steps.

5. Authority

a. Exceptions to this Policy may be made by the Co-Chairs of the PCI DSS Steering Committee (the CTO or CFO) on the recommendation of the Committee. The Vice President (Administration), upon advisement by the Co-Chairs (CTO and CFO) of the PCI DSS Steering Committee, has the authority to grant exceptions to this Policy

A decision to suspend a Merchant due to Non-Compliance to this Policy may be made by the Co-Chairs of the PCI DSS Steering Committee (the CTO or CFO) on the recommendation of the Committee.

E. Related Procedures or Documents

- Information Security Policy
  https://informationsecurity.mcmaster.ca/wp-content/uploads/2017/06/Information-Security-Policy.pdf

- Fraud Policy
  https://www.mcmaster.ca/vpadmin/Policies/IAPolicy_Fraud.pdf

- Statement on Collection of Personal Information and Protection of Privacy
  https://secretariat.mcmaster.ca/app/uploads/2019/06/FIPPA_Statement.pdf

- Cash Control Policy and Procedures
  https://financial-affairs.mcmaster.ca/app/uploads/2018/07/Cash-Control-Policy-and-Procedures-.pdf

- List of approved Payment Provider and External fees (*contact Financial Affairs*)

- Procedures for Acceptance of Payment Cards and eCommerce Payments
  https://financial-affairs.mcmaster.ca/app/uploads/2018/07/Procedures-for-the-Acceptance-of-Payment-Cards-and-E-Commerce-Payments.pdf

- Terms of References
  https://financial-affairs.mcmaster.ca/app/uploads/2018/07/PCI-DSS-Steering-Committee-Terms-of-References-revised-November-21-2018.._.pdf