McMASTER UNIVERSITY

Complete Policy Title: POLICY FOR ACCEPTANCE OF PAYMENT CARDS

Approved by:	Vice President, Administration
Date of Most Recent Approval:	November 2011
Effective Date:	1 December 2011
Related Policies:	Information Integrity and Security Policy Dishonest or fraudulent activities related to funds or property owned by or in the care of McMaster University. Statement on Collection of Personal Information and Protection of Privacy. Cash Control Policy and Procedures
Position Responsible for (i) Developing:	Director, Finance IT Security Officer, University Technology Services
and (ii) Maintaining the Policy:	**Assistant Vice-President (Administration)** **Chief Information Officer**
Contact Department:	**Assistant Vice-President (Administration)**

DISCLAIMER: *If there is a discrepancy between this electronic policy and the written copy held by the Policy owner, the written copy prevails.*

1. PREAMBLE

1.1 The Payment Card Industry ["PCI"] has established industry standards for the processing of purchase transactions electronically. The acceptance of debit and credit Payment Cards ["Cards"] provides a convenient way to process purchase transactions [i.e., sale of goods and services, registration fees].

1.2 It is critical that the process for accepting, processing and storage of information relating to Card transactions be secure to (i) protect the privacy and personal information and (ii) safeguard Card users' bank accounts and other assets.

1.3 All Merchants/Departments/Faculties ["Departments"] must meet the University's requirements for security and for integrating transaction information into the University's systems.

1.4 Departments wishing to accept payment cards should complete the application at the bottom of this policy using the process flow outlined. Applications are jointly reviewed by Financial Services and UTS Security before processing privileges are granted. Once approved payment processor contact numbers and merchant number(s)

will be assigned.

2. SCOPE

2.1 This Policy is applicable to all Departments and affiliates with active McMaster Merchant numbers and all Departments wishing to/or currently processing Payment Card transactions by way of any of the following methods:

- website [eCommerce],
- entered by staff from information provided by a Card user [i.e., fax, telephone]
- point of sale ["POS"] terminals,
- Third-party hosted services

2.2 Separate legal entities processing Payment Card transactions and whose systems reside on the McMaster network must attest they meet the PCI requirements as per Section 5 of this Policy.

3. DEPARTMENT RESPONSIBILITIES

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

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

3.3 Departments are responsible for retaining the appropriate transaction records for audit purposes for a period of seven years.

3.4 Departments must comply with the University Statement on Collection of Personal Information and Protection of Privacy.

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

3.6 Departments must adhere to the Data Incident Policy.

3.7 All Department staff must be cognizant of the University's Dishonest or fraudulent activities related to funds or property owned by or in the care of McMaster University (the Fraud Policy) and conduct their affairs accordingly.

3.8 Departments are responsible for all fees both internal and external. These will be charged to the department though standard journals up loaded on a regular basis.

4. HOSTED AND OUT-SOURCED SERVICES

Prior to entering into a business arrangement with a third-party vendor, the McMaster Department will provide written confirmation the third-party meets the following requirements:

4.1 The vendor is liable for all potential or real security breaches and costs associated with Payment Card Processing and will indemnify McMaster for all costs incurred by McMaster associated with such a breach. Suggested Contract wording is:

> The vendor acknowledges in writing that any potential, threatened or actual security breach, inadvertent release of confidential information or malfunction of the McMaster University Payment Card System ("Breach") arising from the vendor's (or from anyone for whom the vendor is at law responsible) actions, omissions, and/or negligence may cause irrevocable economic, consequential and/or punitive damages, losses, claims, fines, costs, demands, penalties, charges, withdrawal of services and/or the incurrence of extensive remedial costs of rectification ,both direct and indirect ("Claims") to McMaster

University and it entire Payment Card System; and the vendor shall covenant and agree to fully indemnify McMaster University from all Costs incurred by it associated in any way with such Breach including without limitation, all Costs associated with professional serviced required by McMaster University to rectify, remedy and satisfy all such Claims

4.2 The Departments must obtain:

4.2.1 A current PCI Certificate of Compliance from the vendor, or

4.2.2 Written attestation from the vendor to the use of a VISA Certified Payment application (https://www.pcisecuritystandards.org/security_standards/vpa/) and provide information on the specific product and version of the software being used for McMaster payment processing

4.3 Within the contract terms, the Department must also obtain agreement from the vendor:

4.3.1 To provide notification of a potential or real breach of their systems to McMaster IT Security (c-it-security@mcmaster.ca)

4.3.2 That McMaster University may cancel the contract upon a security breach occurring.

4.3.3 The vendor report to McMaster University if their systems become non-compliant,

4.4 If a McMaster Merchant number is to be used, then the third-party vendor must also meet the following requirements within the contract terms:

4.4.1 McMaster University reserves the right to audit the third-party vendor with respect to security of the payment card processing and associated systems and data, with 10 business days' notice.

4.4.2 At the request of McMaster, the third-party vendor will submit a copy of the latest quarterly scan performed on their payment processing systems, in accordance with PCI-DSS.

4.5 The Terms of any contract with a third-party vendor will meet those outlined in this Policy.

5. SECURITY STANDARD PROCEDURES

5.1 The PCI Security Council has established 6 elements required for every merchant that processes Card transactions as follows:

1) Build and Maintain a secure network

2) Protect Cardholder Data

3) Maintain a Vulnerability Management Program

4) Implement Strong Access Control Measures

5) Regularly Monitor and Test Networks

6) Maintain and Information Security Policy

The majority of these requirements apply to electronic storage, processing and transmission of cardholder data; however; all Card processing is assessed against these standards.

5.2 The University does not allow the use of e-mail to initiate and/or effect a transaction as this method would involve transmission of sensitive information in an unsecured manner and environment

5.3 Departments with an active merchant number may be subject to an external security audit, at the expense of the department.

6. COMPLIANCE

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

6.2 The suspension process of the merchant number account includes:

- Notification from a vulnerability scan and/or internal audit of a breach of PCI requirements and/or lack of adherence to this Policy; this notification asks that remedial action be taken and for the Department to report back.
- If remedial actions are incomplete and/or an undue time elapses without resolution of the issues, a final request for compliance with an expectation the Department provides a written plan indicating who is resolving issues and by when.

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

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

6.5 Each Department Account Signing Authority must attend the annual training and attest as to compliance with this policy annually when notified by PCI Steering Committee that such attestation is due.

6.6 The Vice President (Administration), upon advisement by the Co-Chairs (CIO and CFO) of the PCI Steering Committee, has the authority to grant exceptions to this Policy.

7. AUTHORITY

7.1 Exceptions to this Policy may be made by the Co-Chairs of the PCI Steering Committee (the CIO or CFO) on the recommendation of the Committee.

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