POLICY NAME	**MERCHANT (PCI) POLICY & PROCEDURES - ACCCEPTING CREDIT/DEBIT CARD PAYMENTS**

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

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 Rete

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.

PR2.2.

The PCI Compliance Steering Committee is:

a) Responsible for McGill's interpretation and communication of PCI Compliance guidelines.

b)

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).