McGill Merchant Manual

The McGill Merchant Manual is a complementary document to the Merchant (PCI) Policy and Procedures and serves to aid Merchants in ensuring their operations comply with Payment Card Industry (PCI) Standards. It was developed as an easy-to-use reference document and includes key PCI requirements as well as operational processes and practices that Merchants must implement to ensure compliance with PCI standards.

Merchants are also responsible for reading and applying the directives provided by the Payment Processing Vendor (e.g. Moneris) in the operational manual.

The Merchant (PCI) Policy and Procedures can be found at: http://www.mcgill.ca/financialservices/policies/

Contents

I. Understanding Payment Card Industry Requirements

1.0 PCI-DSS

Payment Card Industry – Data Security Standards (PCI-DSS) are standards developed by the PCI Security Standards Council. The PCI Security Standards Council is a security council founded by the five major credit card providers: American Express, Visa Inc., MasterCard Worldwide, Discover Financial Services, and JCB International.

PCI-DSS is the authorized program of goals and associated security controls and processes that keep payment card data safe from fraudulent use.

2.0 Why McGill Needs to Comply?

McGill needs to comply because cardholder data is sensitive, and criminals can easily unlock direct access to money and personal identities. Statistics indicate that the number of attacks on payment card processing systems is rising, and the most vulnerable sector for data breaches is the Merchant population.

3.0 Risks of Non-Compliance

If McGill merchants do not comply with PCI-DSS standards, this could result in the entire University's (all merchants) inability to accept and process future card payments. The University's reputation would be at risk, and customers, in particular our students and donors, would lose confidence in the University's systems and processes. This could potentially lead to lost revenues, and the University could be required to pay penalties or absorb the cost of legal settlements.

4.0 Who Needs to Comply?

In the eyes of PCI Compliance, one institution is equal to one merchant. Certification is at the institutional level. In order for the University to be compliant, all merchants must comply.

5.0 Cardholder Data Elements

6.0 Who is a Merchant?

You are a merchant if your unit accepts credit and/or debit cards for the sale of goods and/or services, for receiving donations, or for any other purpose. Your unit may have one or more than one type of merchant:

a. E-Commerce merchants

The cardholder makes a payment, deposit, or donation over the internet through a website, an app, or any other interface, and is prompted to enter a credit card number, expiration date, and card verification code or value. The purpose of the card verification code or value is to ensure that the cardholder has the credit card in hand. The payment is considered processed when an authorization code or message is displayed on the screen.

b. Stand-alone Terminal (PINPad) merchants

The cardholder must insert or swipe the card in the PINPad in order to make a payment, deposit, or donation. The Terminal (PINPad) is not integrated with a cash register / software / hardware, and the credit card information cannot be captured in the cash register / software / hardware. The payment is considered processed when an authorization code is returned to the merchant.

c. Point of sale (POS) merchants

The cardholder (or employee) must insert or swipe the card in the PINPad (or integrated card reader) in order to make a payment. The Terminal (PINPad) is integrated with a cash register / software / hardware. The payment is considered processed when an authorization code is returned to the merchant.

d. IVR merchants

Without an internet solution or a physical terminal, the IVR merchant enters the credit card information (primary account number, expiry date, and transaction amount) via the University's contracted vendor payment processing automated phone system to process the payment. The use of soft phones (i.e. telephone software, Skype, etc.) is not permitted. If the cardholder is present, the merchant will use the imprinter to make an impression of the credit card along with the cardholder signature as proof of payment.

II. Operational Requirements

1.0 Paper, Records Retention, Scanning, and Disposal Requirements

a) Paper

Examples of paper documents that may contain sensitive cardholder data elements are: customer order forms, course registration forms, reports, supporting documentation (receipts or invoices), imprinter sales drafts, and proof of payment.

- If course registration or customer order forms contain fields for credit card information, the form must clearly indicate that it can only be faxed to the merchant's fax number or delivered in person (if applicable). You can include the following disclaimer: For security reasons, please do not send your credit card information electronically (email, instant message, scanned document, etc.). To fax this form, please send it to fax number: (999) 999-9999 or bring it to the following address: 1234 Main Street, suite 9999, Montreal (QC) X9X 9X9.
- Credit card information must never be transmitted electronically (i.e. email, scanned and emailed, instant messaging). Please see Section II, subsection 3.0 for more information on receiving credit card information by fax.
- Reports with credit card information MUST NEVER be printed.
- The card verification code value (CVV) must never be collected on any document.

b) Records Retention

If the supporting documentation and/or proof of settlement contains cardholder data and must be retained, the Merchant must:

a. Black out the primary account number (PAN) (the first 6 and last 4 digits of the number may remain visible).
b. Photocopy the document that has the PAN blacked out.
c. Shred the original document.
d. Retain only the photocopied document.

Supporting documentation must generally be retained for seven years (*please refer to the McGill University Records Retention Schedule*). Proof of settlement can only be stored for a period of 18 months for the sole purpose of responding to disputes. Proof of settlement must be destroyed immediately after this time.

c) Scanning: If you are scanning any documents that contain cardholder data, the primary account number (PAN) must first be blacked out (the first 6 and last 4 digits of the number may remain visible). Once your documents are scanned and saved on the network, the original documents must be shredded.

d) Disposal requirements are as follows:

- If documents that contain cardholder data are shredded, the shredder must cross-cut or micro-cut. If the shredder stores paper prior to shredding, the container must be securely locked.
- If documents that contain cardholder data are transported, the boxes must be sealed.
- If documents that contain cardholder data are handled by another service provider (e.g. transporter, shredding company), the service provider must be PCI-DSS compliant.
    - On the New Merchant Questionnaire, you will be asked to identify the name of the service provider which will be validated by Banking Services and Financial Services.

2.0 Electronic Storage of Cardholder Data

McGill University DOES NOT allow the electronic storage of cardholder data. Cardholder data cannot be stored, transmitted, or received by electronic means (except by fax; see Section II, subsection 3.0). This includes systems, databases, application, and networks.

3.0 Receiving Cardholder Data by Fax

If you receive Cardholder Data on documents via fax, the fax must either be a dedicated fax machine, in a controlled environment or if it is a shared fax machine, then it must have an identification functionality (i.e. password must be typed in to release the document or a McGill ID must be swiped).

If the form is received by another service provider, the provider must be PCI-DSS compliant.

4.0 Systems

If you are developing or purchasing a system or application to support your payment process, it must be vetted by Information Technology Services to ensure PCI Compliance requirements are met. Furthermore, if your intent is to purchase a system or application, PCI Compliance must be incorporated as a key criterion in any tendering document.

5.0 Standalone Terminal (PINPad) / Point of Sale (POS) Merchants AND Administration Cards

Administration Cards are issued to these merchants in order to process refunds and certain reports that could contain cardholder information. It is recommended that these Administration Cards be restricted to the Supervisor or Unit Head. If it cannot be, then the Supervisor or Unit Head should at least ensure that a segregation of duties is maintained. This translates to: employees should not be authorized to process refunds for payments they have processed. The Administration Card should be physically secured when not in use, and it should never be shared. The Supervisor or Unit Head should use the Payment Processing Vendor's reports to monitor and reconcile refund transactions.

6.0 Processing Refunds and Refund Policy

- Refunds must always be processing using the same method as the payment. In other words, credit card refunds must be made to the same credit card as the payment; debit card refunds must be made to the same debit card as the payment. Payment card transactions should never be refunded by cash or cheque.

- Segregation of duties should be implemented: individuals should not be authorized to process refunds for payments they have processed.

- Only McGill employees should be authorized to process refunds.

- Supervisors or Unit Heads should be responsible for monitoring refunds through Merchant Direct.

Refund Policy

- The *payment processing vendor* requires the following:
    - For e-commerce merchants, the refund policy must be clearly indicated on the website.
    - For all stand-alone PINPad and POS merchants, the refund policy must be visible to the customer (e.g. displayed at the counter).
    - For IVR merchants, the refund policy must be indicated on the payment form.

7.0 Reviewing Sales and Refunds

The Supervisor, Unit Head or Fund Financial Manager is responsible for ensuring that their financial statements adequately reflect all sales and refunds. To do so, the Supervisor, Unit Head or Fund Financial Manager should reconcile the financial statements to the subsystem or registration system.

8.0 E-Commerce Merchants and Processing Payments

Access to payment functionality through the Merchant Resource Centre/Virtual Terminal (allowing merchants to process online payments on the customer's behalf) will only be granted if a valid business case is presented and no other viable option is available.

You must advise the PCI Compliance Steering Committee if:

- You intend to allow your customer/donor to use your desktop/laptop to make a payment, deposit or donation on your website.
- You intend to collect credit card information over the phone from your customer/donor in order to process the payment, deposit or donation through your website on your customer's/donor's behalf.

Processing the payment or donation through your desktop / laptop renders your computer subject to PCI-DSS standards.

Please communicate with Banking Services before selecting a website developer.

9.0 Transfers and Terminations

You must advise the Banking Supervisor, Banking Services when:

- an employee who has access to your **IVR** system has transferred out of your unit or left the University;
- an employee who has access to your Merchant Resource Centre/Virtual Terminal has transferred out of your unit or left the University; the employee's Merchant Resource Centre/ Virtual Terminal account must also be deactivated.

10.0 Non-McGill Staff or Service Providers Involved in the Merchant Process

If you have non-McGill Staff (e. g. volunteers, web designers, third-party vendors, etc.) involved in your merchant process, then:

- Avoid giving them access to paper documents or electronic media that contain cardholder data.
- If access is required, then the Supervisor or Unit Head must:
    - Ensure that there are sound work processes and training programs in place to ensure compliance.
    - Ensure that non-McGill staff have read and understood the Merchant (PCI) Policy and Procedures and the Merchant Manual.

If Service Providers are involved in your merchant process, they must be PCI-DSS compliant.

- The New Merchant Questionnaire will ask you to identify the names of all service providers, which will then be validated by Banking Services, Financial Services.

11.0 Sharing of IDs and Passwords

As a merchant, you must ensure that there is no sharing of IDs and passwords, since these IDs and passwords provide access to card processing applications and reporting (i.e. Merchant Direct, Merchant Resource Centre/Virtual Terminal, etc.). This is also consistent with the Code of Conduct for Users of McGill Computing Facilities.

Key Contact

- Banking Supervisor, Banking Services: 514-398-3353
- To report any incident, fraud, or breach, please contact the PCI Compliance Steering Committee: PCIComplianceSteeringCommittee@campus.mcgill.ca

Links to Related Documentation

- Merchant (PCI) Policy and Procedures: http://www.mcgill.ca/financialservices/policies/merchant

- Moneris: http://www.moneris.com/
- Moneris Merchant Direct: https://www1.moneris.com/cgi-bin/rbaccess/rbunxcgi?F6=1&F7=L8&F21=PB&F22=L8&REQUEST=ClientSignin&LANGUAGE=ENGLISH

- Merchant Resource Centre: https://www3.moneris.com/mpg/index.php