PAYMENT CARD STANDARDS

PURPOSE

A standard includes specific low level mandatory controls that help enforce and support a policy.

The purpose of this document is to support and outline in detail the requirements of the Payment Card Policy. These requirements are mandatory and must be adhered to by all University areas / departments ("merchants") accepting debit / credit cards.

PIN Transaction Security device

See **Appendix A** for leading practices issued by the PCI Security Standards Council related to securing PIN Transaction Security (PTS) devices.

Only approved PTS devices from the acquirer must be used by University merchants (see https://www.pcisecuritystandards.org/assessors_and_solutions/pin_transaction_devices).

Wireless PTS devices that use the University's wireless network are not permitted under any circumstance; only GSM cellular or analog phone-enabled PTS devices are permitted.

PTS device - new

An area / department requiring a new PTS device must first arrange with Financial Services to obtain a merchant account. Specifically, the area/ department must submit a request to Financial Services, with a copy to the AVP, Financial Services and pcisecurity@brocku.ca .

Once the merchant account has been obtained, Financial Services will arrange with the acquirer (currently Chase Paymentech) for a new PTS device, and will inform the requestor when the PTS device is received.

Upon receipt of the new PTS device, the requestor must take pictures of the front and back of the unit as well as the unit's serial number and the phone jack, including the phone jack number where the unit will be connected. The PTS device application version must also be noted. All pictures and information must be submitted to pcisecurity@brocku.ca to update the PTS device inventory for the University (see PTS device – inventory below).

PTS device - replacement

An area / department requiring a replacement PTS device must submit a request to Financial Services, with a copy to the AVP, Financial Services and pcisecurity@brocku.ca. Financial Services will arrange with the acquirer (currently Chase Paymentech) for a replacement PTS device, and will inform the requestor when the PTS device is received.

Upon receipt of the replacement PTS device, the requestor must take pictures of the front and back of the unit as well as the unit's serial number and the phone jack, including the phone jack number where the unit will be connected. The PTS device application version must also be noted. All pictures and information must be submitted to pcisecurity@brocku.ca , including information on the PTS device which is being replaced.

The PTS device inventory will be updated accordingly (see PTS device – inventory below).

PTS device - returns

An area / department wishing to return a PTS device must do so through Financial Services, with a copy to the AVP, Financial Services and pcisecurity@brocku.ca .

The PTS device inventory will be updated accordingly (see PTS device – inventory below).

PTS device – inventory

The University's PTS device inventory is maintained centrally. All changes to PTS devices (new / replacement / returns) must be communicated by the area/ department to pcisecurity@brocku.ca in a timely manner in order for the inventory to be kept current.

PTS device - security

PTS devices must be treated as cash: where possible, they should be kept secured and out of sight when not in use. This includes backup PTS devices which may not be used as frequently.

Where possible, the terminal and PTS device wires must be secured by bolting wire cabling to the PTS device and terminal. This will deter fraudsters from stealing the PTS device and terminal and make it more difficult to plant a compromised unit. An alternative is to use a secure stand in which the PTS device is bolted and wiring is not easily accessible.

Areas / departments should consider placing an identifying mark or sticker on the back or in a visible area of the PTS device in order to facilitate verification that the PTS device has not been swapped with a compromised unit.

The identity of any technician who arrives to service any payment card-related equipment must be validated prior to commencement of any work. Non-scheduled in-person contact by a third party with any Brock-leased payment card-related equipment must not be permitted.

The most current version of the payment application software should be in use as older versions may lack adequate functionality to facilitate PCI DSS compliance.

PTS device - inspection

PTS devices must be regularly inspected. The inspection frequency may range from daily reviews for areas / departments with high transaction volumes to monthly / quarterly reviews where there is less traffic and / or the PTS device is maintained in a secured location (e.g., locked office). A log of each review must be maintained (see **Appendix B** for an example).

Each area must appoint a person who is responsible and independent to conduct the periodic PTS device inspection and update the log. If the PTS device is compromised or substituted, the log will aid in the investigation.

The physical inspection must consist of a review of the following at minimum and must be documented (see **Appendix B** for an example of an inspection log):

- PTS device make, model and serial number;
- Security stickers to ensure they are intact;
- Connection cable to ensure that it has not been tampered;
- Physical security to ensure that the PTS device cannot be removed.

Card not present transactions

If paper forms are used for card-not-present transactions (e.g., telephone and mail order) and retention of a section of the form is necessary, then the cardholder data section of the payment form must be removed and cross-cut shredded. For mail order card-not-present transactions, ensure that the signature portion of the form is retained.

Recurring transactions

If cardholder data is required to be retained for recurring transactions (e.g., monthly membership fees, rental payments, donations, etc.), your requirements / proposed process must be discussed beforehand. Contact pcisecurity@brocku.ca prior to retaining cardholder data.

Cardholder data received via email / voicemail / social media

Transactions related to cardholder data received via email / voicemail / social media must not be processed and must be immediately and permanently deleted in a secure manner.

The cardholder must then be informed that cardholder information received via insecure means such as email / voicemail / social media cannot be processed, and an alternative means of payment discussed (e.g., telephone, in person).

Front line employees who typically deal with payment card transactions must update their email signature block to include the following statement: "*Please do not send credit or debit card information via email. Credit or debit card information received via email will not be processed and will be immediately and permanently deleted.*"

Front line employees who typically deal with payment card transactions must update their voicemail message to include the following statement: "*Please do not leave credit or debit card information on voicemail. Credit or debit card information left on voicemail will not be processed and will be immediately and permanently deleted.*"

Cardholder data received via telephone

Procedures for accepting cardholder data via telephone can be found in **Appendix C**.

Paper notes may be used to temporarily capture cardholder data received over the telephone. The transaction must be processed immediately, and the paper notes with cardholder data must be securely destroyed (e.g., cross-cut shredded) once the transaction is completed.

Processing refunds

Procedures for processing refunds can be found in **Appendix D**.

Cardholder data via fax

If a fax machine is used to receive cardholder data, the fax machine should be a stand-alone machine placed in a secured location. The fax machine must have minimal memory and be connected via an analog phone line.

Cardholder data received via fax must be processed immediately, and the faxed printout with cardholder data must be securely destroyed (e.g., cross-cut shredded) once the transaction is completed. For fax transactions, ensure that the signature portion of the form is retained.

Payment applications

Software classified as a payment application must be compliant with the Payment Application Data Security Standards (PA-DSS).

A list of payment applications that have been validated as PA-DSS compliant can be found on the PCI website here: https://www.pcisecuritystandards.org/assessors_and_solutions/vpa_agreement .

The specific version number of the payment application must be listed on the PCI website as a Validated Payment Application.

Important to note: "*Use of a PA-DSS compliant application by itself does not make an entity PCI DSS compliant, since that application must be implemented into a PCI DSS compliant environment and according to the* PA-DSS Implementation Guide *provided by the payment application vendor*".[1]

Use of service providers

When initiating / renewing an agreement with a service provider, it is important to first determine whether the services being procured involve the off-site storage, processing or transmission of cardholder data. If so, PCI DSS requirements are applicable. This means that specific reference to PCI DSS compliance is required in the service provider agreement. In addition, on-going monitoring of the service provider's PCI compliance is required.

Only PCI-compliant service providers must be engaged by a University merchant for technologies / solutions related to accepting / transmitting / processing/ storing (note: no on-site storage of payment card data is permitted) cardholder data.

PCI compliant service providers / vendors can be found on the following:

- Visa Global Registry of Service Providers (http://www.visa.com/splisting/);
- Mastercard Compliant Service Provider List (https://www.mastercard.us/en-us/merchants/safety-security/security-recommendations/service-providers-need-to-know.html - available as a download);
- PCI website (https://www.pcisecuritystandards.org/assessors_and_solutions/qualified_integrators_and_resellers).

[1] Payment Card Industry (PCI). Version 3.0 November 2013. Payment Application Data Security Standard, p 5.

A recent / current "Self-Assessment Questionnaire and Attestation of Compliance for Service Providers" is required prior to engaging the service provider, as well as annually thereafter. Furthermore, evidence of successfully passing a vulnerability scan with a PCI DSS Approved Scanning Vendor (ASV) is required.[2]

It is important for these requirements to be reflected in the written agreement with the service provider. The written agreement should also include the service provider's acknowledgement that the service provider is responsible for the security of cardholder data that it stores / processes / transmits on behalf of the University.

In the event of a compromise

If a cardholder data security breach is suspected (see **Appendix E**), the University's IT Incident Response Policy and related IT Security Incident Response Standards must be followed.

The Associate Vice-President, Information Technology Services and / or the Associate Vice-President, Financial Services must be notified immediately. Either will initiate contact with:

- The University's Insurance Co-ordinator. A determination will be made with the insurer whether to involve an external forensics expert;
- The affected credit card company and acquirer:
  - Visa: (416) 860-3090 or CanadaInvestigations@visa.com
  - Mastercard: see https://globalrisk.mastercard.com/wp-content/uploads/2019/08/ADC-Best-Practice-Manual.pdf for information on how to access the *Account Data Compromise Reporting Form* p. 7
  - ChasePaymentech: contact to be facilitated via Financial Services.
- The University's Privacy Co-ordinator;
- Marketing & Communications to initiate a communications plan (see Visa's *Responding to a Data Breach: Communications Guidelines for Merchants* https://usa.visa.com/dam/VCOM/global/support-legal/documents/responding-to-a-data-breach.pdf);

[2] Note: scanning does not apply to all service providers. It is only required for Validation Type 4 and 5, i.e., merchants with external facing IP addresses. If a merchant stores cardholder data electronically or if the merchant's processing systems have any internet connectivity, a quarterly scan by an approved scanning vendor is required

- Director, Campus Security Services, who will assist in determining whether the incident should be reported to the Police.

In the event of a breach or suspected breach, the area / department must immediately execute each of the steps below:

- Document every action taken from the point of suspected breach forward, preserving any logs or electronic evidence available;
- If the affected machine is a desktop or laptop, disconnect the computer/ device(s) from the network. DO NOT turn the system off or reboot. Leave the device powered on and disconnected from the network
    - Prevent any further access to or alteration of the compromised system(s) (i.e., do not log on to the machine and/or change passwords; do not run a virus scan). Leave the system(s) as is, disconnected from the network.

Appendix A: Skimming Prevention: Best Practices for Merchants (issued by the PCI Security Standards Council)

https://www.pcisecuritystandards.org/documents/Skimming%20Prevention%20BP%20for%20Merchants%20Sept2014.pdf

Appendix B: Sample PTS device Inspection Log

Make:	Model number:	Serial number:	Jack number:
General condition and appearance: (colour, existing marks, scratches, etc.)			
Location of manufacturer's security seals or labels:			
How many connections in total (all leads, plugs, aerials, etc.) and description of the connections (type and colour of cables, etc.)?			
Describe the "normal" condition of the ceiling above the PTS device (include scuffmarks, fingerprints, dislodged tiles, etc.).			

Inspection date:					
Inspection time:					
Inspector initials:					
Do the make, model number, serial number and jack number match the information above?					
Is the PTS device in its usual location?					

Are the colour and general condition of the PTS device as described, with no additional marks or scratches (especially around the seams)?					
Are the manufacturer's security seals and labels present, with no signs of peeling or tampering?					
Are the manufacturer's security markings and reference numbers as described?					
Are all connections to the PTS device as described, using the same type and colour of cables, and with no loose wires or broken connectors?					
Count the number of connections to the PTS device. Does this agree with the number stated?					
Is the condition of the ceiling above the PTS device as described, with no additional marks, fingerprints or holes?					
Is the total number of PTS devices in use the same as the number of PTS devices officially installed?					
Comments					

Appendix C: Procedures for accepting cardholder data over the phone

PURPOSE

The purpose of this document is to provide direction on how to accept highly sensitive cardholder data over the telephone. These Procedures must be followed by all University merchants accepting cardholder data over the telephone as outlined in the Payment Card Policy.

Accepting cardholder data over the phone

If a PTS device is close by:

- Directly enter the customer's payment card number and expiry date as prompted on the PTS device. Transfer the call to a phone adjacent to the PTS device if needed. Do not record the payment card data.
- Do not repeat the payment card number or expiry date back to the customer while obtaining the numbers. If you are unsure, ask the customer to repeat some or all of the numbers back to you.
- Keep the customer on the phone while the transaction is being processed and let them know the result as approved or declined.
- Either scan the sales receipt and email it with the invoice to the customer or mail the customer copy of the sales receipt to the customer with a printed invoice.
- Write the customer's first and last names on the merchant copy of the receipt. Store the merchant receipt in the office safe.

If a PTS device is not immediately available:

- Record the payment card data on paper; DO NOT record **any** cardholder information electronically.
- Do not repeat the credit card number or expiry date back to the customer while obtaining the numbers. If you are unsure, ask the customer to repeat some or all of the numbers back to you.

- Determine how the customer wants to be informed of the success of transaction processing (email / voicemail should not be an option).
- Once the transaction is processed, cross-cut shred the paper with the payment card data.
- Either scan the sales receipt and email it with the invoice to the customer or mail the customer copy of the sales receipt to the customer with a printed invoice.
- Write the customer's first and last name on the merchant copy of the receipt. Store the merchant receipt in the office safe.

Processing refunds

- If the payment was made manually via the PTS device, ask the customer to provide the original payment credit card method and follow the procedure for processing phone payments above.
- See **Appendix D: Processing Refunds** for additional information.

Declined or incomplete transactions

- If a transaction is declined, inform the customer accordingly. Explain this may occur due to security features of their credit card or incorrect information.
    - The University accepts VISA, Mastercard and debit cards only. Cards with "for electronic use only" may not be accepted.
    - The same card may be attempted with the customer up to three times.
    - Offer to try a different card if available, or to pay by an alternate accepted method of payment.
    - Ask the customer if they would like to contact their bank before attempting their card again.

- If a transaction is declined do not record the credit card information to try again later.
- If there is a power outage, the machine runs out of paper, or there is another interruption, do not record the credit card information.

Appendix D: Processing Refunds

PURPOSE

This procedure was developed to ensure that all departments are following the same refund process with the appropriate internal controls. This process is also designed to prevent mishandling of funds and to safeguard against loss. A refund should not be provided unless the original receipt is presented.

System requirements

- Refund transactions must be linked to the original sales transactions in the POS system to facilitate the monitoring, analysis and auditing of refunds.
- If possible, one/separate POS terminal is to be dedicated for refunds to restrict access.
- The reason for the return should be documented. If possible, the return reason should be documented in the POS system.

Payment requirements

- Refunds are to be processed using the same method of payment as the original sale.
- If the original method of payment is a card (i.e., debit or credit) the refund must be processed to the card number used in the original purchase. The card number can be identified by comparing the last four digits on the card to the last four digits on the sales receipt.
- If the original credit card has been cancelled or expired, a refund is to be processed on a store/gift card. A refund for the services that require registration (i.e., residence, membership, parking) can also be processed through a cheque requisition instead of a store/gift card. If the refund is for a student, it can also be processed through the student account. Unit management may refund a transaction to a different card used in the original purchase on an exception only basis. The reason for the exception must be documented in the POS system or by other means if not possible in the POS system.

Documentation requirements

- The refund policy must be clearly displayed or communicated to the customer at the time of the initial sales transaction.
- Customers must be provided with a sales receipt at all times.
- Returned items must be circled and flagged as "returned" on a customer's original sales receipt. A cashier processing the return is to write his/her initials next to the returned item.
- Merchant copy of the return receipt must have the following information handwritten by a customer:
  - ✓ Signature
  - ✓ Full name
  - ✓ Phone number

Physical inventory management requirements

- A bin must be dedicated in which the returned items must be placed.
- As part of the daily reconciliation and review process, unit management must reconcile the refunds in the system to the physical items in the bin.
- Spot inventory counts are to be conducted to ensure that the refund is legitimate and a piece of merchandise was not taken off of the shelf and placed in the bin.

Review requirements

- Someone other than the person receiving payments and processing refunds is responsible for a daily review of refund logs/reports.
- Reviewers must ensure the following when reviewing daily refunds:
  - ✓ Refunds tie back to original sales transactions in the system.
  - ✓ Refund payment methods are the same as the ones that were used for the initial sales transactions.
  - ✓ If it is a return of goods, inventory counts are conducted and are to be highlighted on the report.

- ✓ A reviewer's name and signature are to be recorded on the report.
- ✓ If the reviewer is not management, then a manager must sign off on the reviewer's report.

- A copy of the refunds report is to be submitted to Financial Services with a daily deposit.

Note: Financial Services and / or Internal Audit will also from time to time ask to review these controls or perform an audit.

Unit procedures for refunds

- Each unit must have written procedures in place to guide and train staff when it is appropriate to provide a refund.
- Procedures must be regularly reviewed and updated.
- Training is to be conducted for all staff.

Appendix E: Signs that tend to appear when a security breach has occurred

(Ref: what to do if compromised, visa inc. fraud control and investigation procedures)

- Unknown or unexpected outgoing Internet network traffic from the payment card environment;
- Presence of unexpected IP addresses or routing;
- Unknown or unexpected network traffic;
- Unknown or unexpected services and applications configured to launch automatically on system boot;
- Unknown files, software and devices installed on systems;
- Unexplained modification or deletion of data;
- Anti-virus programs malfunctioning or becoming disabled for unknown reasons;
- Excessive failed login attempts in system authentication and event logs;
- Vendor or third-party connections made to the cardholder environment without prior consent and/or a FootPrints ticket;
- SQL injection attempts or strange code in web server logs;
- Authentication event log modifications (e.g., unexplained event logs are being deleted);
- Suspicious after-hours file system activity (e.g., user login or after-hours activity to Point-of-Sale (POS) server);
- Presence of a rootkit, which hides certain files and processes in, for example, Explorer, the Task Manager or other tools or commands;
- Systems rebooting or shutting down for unknown reasons;
- Unexpected file lengths, sizes or dates, especially for system files;
- Unexplained new user accounts;
- Presence of archived/compressed files in system directories;
- Variances in log chronology or timestamps;
- Hidden malicious code in Windows registry.