

Payment Card Processing Manual

Table of Contents

1.	Introduction to Payment Card Processing	2
2.	Payment Card Acceptance at Carleton University.....	2
3.	PCI Compliance Roles at Carleton University	3
4.	Payment Methods and Merchant Account Management.....	4
4.1	Approved Payment Methods.....	4
4.2	Opening a Merchant Account with the Approved Acquiring Bank	4
4.3	Changes to the Merchant Account	4
4.4	Closing a Merchant Account.....	5
5.	Merchant Operations and Responsibilities.....	5
5.1	Written Merchant Operational Procedures	5
5.2	Merchant-Specific Payment Card Data Incident Response Plan.....	6
5.3	Mandatory Training: PCI and Location-Specific.....	6
5.4	Processing and Security Requirements.....	6
5.5	Telephone and Mail Orders.....	8
5.6	Paper Forms with Payment Card Data	9
5.7	Third-Party Service Providers (TPSP)	9
5.8	Annual PCI Compliance Cycle and Merchant Reporting Milestones	10
5.9	When to Proactively Contact the PCI Compliance Officer?	11
6.	References.....	12
7.	Glossary.....	13
Appendix A: Opening a Merchant Account with the Approved Acquirer		18
Appendix B: Closing a Merchant Account.....		21
Appendix C: New Third-Party Service Provider Onboarding Process.....		23
Appendix D: New E-commerce Merchant Location Approval Process.....		26
Appendix E: Deployment and Physical Security of a Virtual Terminal Device		29
Appendix F: Point of Sale Terminal Security Training and Procedures		30
Appendix G: Payment Card Data Security Incident Response Plan: Standalone Cellular & Wired Terminals		31
Appendix H: Payment Card Data Security Incident Response Plan: E-Commerce & Virtual Terminal		32

Last updated June 27, 2025

1. Introduction to Payment Card Processing

This document outlines the minimum requirements for accepting credit and debit card payments at Carleton University. The goal is to protect customers' payment card data, minimize the risk of data breaches, mitigate financial and reputational risks to the University, and ensure compliance with the Payment Card Industry Data Security Standard (PCI DSS). Non-compliance may lead to the loss of card payment privileges.

Before accepting credit or debit card payments, departments should assess the costs and compliance obligations. Costs include setup fees, monthly rental fees, transaction fees, and chargebacks. PCI compliance involves annual training, equipment and systems security, and managing access privileges. Financial infrastructure must be in place to ensure proper reconciliation of transactions.

Contact the [PCI Compliance Officer](#) (Financial Services, Business Operations) to discuss your options.

2. Payment Card Acceptance at Carleton University

Carleton University has established principles and guidelines for accepting payment cards to ensure compliance and security.

Approved Carleton Merchants:

- Only approved [Carleton Merchants](#) (Carleton departments that have an approved merchant account with the university's Acquiring Bank Chase Payments Canada) are authorized to accept credit/debit card payments on behalf of the University. Merchant activities are overseen by Financial Services and facilitated by the PCI Compliance Officer.
- Departments wishing to accept payment cards **long-term** require a merchant account with the University's Acquiring Bank of choice.
- For **short-term** endeavors (e.g., annual or one-time events), departments may use the University's [E-Commerce service](#).

Financial Infrastructure

- All departments accepting credit/debit card payments, whether long- or short-term, require a financial infrastructure for settlement and reconciliation. To request a new Fund, fill in and submit this [form](#). If you have any questions about which type of fund to select, please contact controllersoffice@carleton.ca for a consultation.

Refund Policy

- All departments accepting credit/debit card payments must have a refund policy.

Mandatory Compliance with PCI DSS

- All aspects of accepting payment cards at Carleton must be PCI DSS compliant to maintain the University's ability to accept credit/debit cards. Non-compliance of one of the University's 40+ merchants risks the entire University's capacity to accept card payments.

Acquiring Bank Exclusivity

- All transactions must be processed through the University's approved acquiring bank Chase Payments Canada.
- Any exceptions need a business case and a formal exclusivity waiver. The exclusivity may be waived if the Merchant needs a product/platform not certified by the Acquirer, and the Acquirer cannot provide an equivalent in a reasonable timeframe. The Merchant must give at least 60 days' written notice.

3. PCI Compliance Roles at Carleton University

Carleton University has established comprehensive requirements and responsibilities for payment card processing to ensure compliance with PCI DSS and protect payment card data.

Merchant Units:

- Adhere to the PCI standards and university policies.
- Complete annual training on payment card data protection.
- Maintain current merchant operational procedures and PCI incident response plans.
- Participate in the university's annual PCI compliance cycle.

The PCI Compliance Team and Financial Services:

- Facilitate PCI-compliant merchant solutions.
- Provide training on security risks and payment card data protection.
- Oversee the university's annual PCI compliance cycle and industry attestation.
- Maintain policies and procedures to govern merchant operations at Carleton University.

Information Technology Services (ITS):

- Secure the University's networks and servers in scope of PCI DSS.
- Promote security awareness.
- Investigate and resolve suspected data breaches.
- Maintain policies and procedures to govern information security at Carleton University.

4. Payment Methods and Merchant Account Management

4.1 Approved Payment Methods

Carleton University supports the following methods for processing credit and debit card payments:

Payment Method	Payment Equipment	Initiated By	Completed By	Additional Notes
Card Present, CP (in-person)	Approved POS terminals	Merchants	Customers	Standard in-person transactions.
Card Not Present, CNP - Telephone Order (TO)	Approved POS terminals or Virtual Terminal devices	Merchants	Merchants	Telephone orders processed by merchants.
Card Not Present, CNP - E-commerce	Customer devices	Customers	Customers	Merchants are not involved except to void or refund.

4.2 Opening a Merchant Account with the Approved Acquiring Bank

To set up a merchant account with the approved acquirer at Carleton University, departments must identify their requirements, resource needs, and consider if a Third-Party Service Provider (TPSP) is necessary.

This involves consulting with Financial Services for fund advice and coordinating with the PCI Compliance Officer for merchant type and equipment.

The process might include onboarding TPSP, ensuring secure POS device deployment, testing the e-commerce solution, securing the virtual terminal setup, completing necessary documentation, and mandatory PCI training.

Finally, the PCI Compliance Officer will submit the Merchant ID request for approval and ensure all systems are ready for operation.

For detailed instructions on each step, please refer to [Appendix A: Opening a Merchant Account with the Approved Acquirer](#).

Merchant accounts are required to be opened for at least 12 months.

4.3 Changes to the Merchant Account

Any changes to a live payment processing environment, including restart of merchant operations following a confirmed security incident/breach, must be validated against PCI DSS and re-approved by ITS Security and PCI Compliance Officer prior to the changes being placed in production.

For e-commerce, all changes must be formally re-approved by the AVP Financial Services.

4.4 Closing a Merchant Account

The process for closing a merchant account involves several steps, including requesting the closure via email to the PCI Compliance Officer, decommissioning POS terminals and e-commerce or virtual terminal portals, removing public access to payment pages, disabling user accounts and PCI network ports. The PCI Compliance Officer will ensure the account is closed and billing discontinued.

For detailed instructions on each step, please refer to [Appendix B: Closing a Merchant Account](#).

Additional Resources for Merchants (Templates and Infographics):

POS Terminals	Appendix F: Point of Sale Terminal Security Training and Procedures
E-commerce	Appendix D: New E-commerce Merchant Location Approval Process
Virtual Terminals	Appendix E: Deployment and Physical Security of a Virtual Terminal Device
TPSP	Appendix C: New Third-Party Service Provider Onboarding Process
PCI Incident Response Plan	Appendix G: Payment Card Data Security Incident Response Plan: Standalone Cellular & Wired Terminals Appendix H: Payment Card Data Security Incident Response Plan: E-Commerce & Virtual Terminal

5. Merchant Operations and Responsibilities

5.1 Written Merchant Operational Procedures

Departments accepting credit/debit card payments must document their merchant operational procedures. Additional to requirements for written procedures documented in the Cash/Cash Equivalent Handling Procedures, written Merchant operational procedures must include, as a minimum:

- **Accepted payment types/cards:** Specify accepted payment types/cards (e.g., Visa, Mastercard, etc.).
- **Approved Payment Methods:** Outline approved methods of processing payments (e.g., in-person, Telephone Orders, e-commerce, virtual terminal, or a combination of these options).
- **Access Protocols:** Define protocols for granting access to merchant systems and equipment. Evidence of account approval, termination and disabling must be available when required for auditing purposes.
- **Telephone and Mail Orders:** Develop protocols for processing Telephone and [Mail Orders](#).
- **Paper Records Management:** Set protocols for secure storage and timely destruction of paper records with payment card data.

- **PCI Training:** Establish protocols to ensure timely completion of PCI training by merchant staff and supervisors/managers.
- **Location-Specific Training:** Develop protocols for location-specific security awareness training for staff upon hire and periodically thereafter. Include training on staff responsibilities during an incident response.
- **TPSPs:** Develop protocols for engaging third-party service providers.
- **Payment Environment Changes:** Create protocols for managing changes to the payment environment.
- **Financial Reconciliation:** Detail financial reconciliation and reporting procedures.
- **P2PE Procedure:** Merchants with Point-to-Point Encryption (P2PE) solution(s) must have documented procedures based on the P2PE Instruction Manual (PIM) and must be able to produce these documents for auditing purposes.

5.2 Merchant-Specific Payment Card Data Incident Response Plan

All merchants must have a location-specific incident response plan aligned with the university's [Payment Card Data Security Incident Response Plan](#). Merchant Leads must appoint an incident response lead and deputy, ensure staff are aware of the plan, and post the applicable 'Print and Post for Staff' document(s).

5.3 Mandatory Training: PCI and Location-Specific

All staff with access to the Cardholder Data Environment must complete PCI compliance training upon hire and annually. Training types include Merchant Training for front-line staff, Supervisor and Merchant Training for supervisory positions, and Technical Training for technical leads.

Location-specific training on the physical security of POS terminals is also required, and must cover the following:

- verification of third-party personnel before granting them access to modify or troubleshoot devices,
- procedures to ensure devices are not installed, replaced, or returned without verification,
- awareness and reporting of suspicious behavior as well as device tampering or substitution.

5.4 Processing and Security Requirements

Carleton University has established universal processing and security requirements to ensure compliance with PCI DSS and protect payment card data.

Universal Processing Rules

- **Currency:** All credit/debit transactions must be processed in Canadian dollars.
- **Processing Costs:** The merchant department is responsible for all charges and fees related to credit/debit card processing.
- **Settlement and Reconciliation:** Merchant departments must reconcile, settle, and report daily.
- **Refunds:** Evidence of the original sale is required. Refunds must not exceed the amount of the original purchase and should be processed to the card used in the original sale. If the original card is no longer

available, a refund must be processed to a different card of the same brand.

If a refund is declined, merchants must contact the Acquirer, document the Acquirer's response, and contact the PCI Compliance Officer before seeking alternative refund options.

Security Requirements

Merchants are responsible for creating an operational and physical environment that complies with PCI DSS, university policies, and privacy laws.

- **Data Sensitivity:** Treat payment card data as "Sensitive" or "Confidential" according to the University's [Data Protection and Risk Management Policy](#).
- **Restrict access to full PAN:** Ensure that Primary Account Number (PAN) is masked on receipts and reports so that only last four digits are displayed.
- **Limit Access:** Limit access to merchant equipment and systems to staff with current PCI training on a [need-to-know basis](#), and revoke access when no longer necessary.
- **Escort Unauthorized Personnel:** Escort unauthorized personnel in areas where payment card data is being processed or stored.
- **Use Unique User Accounts and Strong Passwords:** Use unique user accounts with strong, secure passwords. Maintain a list of all users (merchant and service provider staff). Ensure passwords/passphrases comply with the [University Information Technology \(IT\) Security Policy](#).
- **Prohibit Electronic Transmission:** Payment card data must never be transmitted via any form of electronic communication (e.g., email, fax, or text).
- **CVV for CNP Transactions:** CVV is mandatory for Card-Not-Present (CNP) transactions (except Mail Orders).
- **Physical Security:** Keep POS terminals and VT devices out of reach of passersby and never leave them unattended. Store them securely and ensure they have access to power and the PCI network (if wired) for security updates.
- **Secure PCI Network:** Use Carleton's secure PCI network for wired POS terminals and VT devices. Place PCI network jacks in areas not accessible to public, protect PCI network ports from unauthorized access, and decommission them when no longer needed. Record and update locations, serial numbers of PCI network ports, and POS terminals' MAC addresses, then share with the PCI Compliance Officer.
- **Approved Network Types:** Cellular and [PCI networks](#) only. Wireless POS terminals must use cellular networks, while wired POS terminals must connect to the university's PCI network. P2PE terminals are an exception. Due to security considerations, Wi-Fi and Bluetooth connections are prohibited.
- **Terminal Inspections:** Inspect POS terminals daily for signs of tampering or substitution; log inspections and submit them to the PCI Compliance Officer quarterly. See [Appendix F: Point of Sale Terminal Security Training and Procedures](#) for more information.
- **Prohibit Manual Keying for Card-Present Transactions:** Do not manually key in card information for card-present (CP) transactions if the card's chip or magnetic stripe is not working; request an alternative method of payment if a card is not working.
- **Protect Voids and Refunds:** Protect voids and refunds with passwords. Staff with void/refund privileges must have unique user accounts for these functions on their POS terminals.
- **Comply with P2PE Manual:** Comply with the P2PE Instruction Manual (PIM) for P2PE terminals,

including physical security and regular inspection reports, in addition to daily PCI DSS compliance inspections.

- **E-commerce Security Measures:** To mitigate risks, implement CAPTCHA, mandatory CVV, and CVV filters. If e-commerce or virtual terminal portals will be inactive for an extended period, either disable the portal and close the associated merchant account or temporarily disable all user accounts. Merchants choosing the latter option remain responsible for all applicable expenses.
- **Non-permanent Locations:** Use only cellular or P2PE POS terminals to process payments at non-permanent locations.

5.5 Telephone and Mail Orders

Telephone Orders

Confirm a business need with the PCI Compliance Officer. Adhere to strict security guidelines for Telephone Orders:

- **Secure Protocols:** Develop protocols for the secure acceptance of Telephone Orders and ensure that merchant staff are aware of and compliant with the procedures.
- **Direct Entry:** Key payment card data directly into an approved POS terminal or VT device without storing it.
- **Approved POS Terminals or VT Devices Only:** Payment card data must never be entered via keyboard on non-secure workstations. The Campus Network, to which all university workstations are connected, is not designed to transmit payment card data securely. Contact the PCI Compliance Officer if you wish to use a Virtual Terminal.
- **No Voice Recording:** Do not use telephone numbers that employ voice recording technology such as voicemail or call quality systems for Telephone Orders. If voicemail cannot be disabled for operational reasons, record a message instructing callers not to leave their payment card data via voicemail.
- **No Call Transfers:** Never transfer Telephone Order calls to another VoIP extension or an external number (e.g., a cell phone).
- **VoIP Restrictions:** Do not use VoIP phones for accepting Telephone Orders off-premises (e.g., while working remotely) as this would pull non-university network into the University's PCI scope.
- **Cell Phone Use:** Cell phones are allowed and can be used to accept Telephone Orders off-premises. Voicemail rules must be complied with.
- **VoIP Inventory Maintenance:** Maintain an inventory of the University's VoIP extensions used to accept Telephone Orders and communicate any changes to the PCI Compliance Officer.
- **Confidentiality:** Be aware of their surroundings when processing Telephone Orders and keep customers' information confidential (e.g., do not repeat the PAN and the CVV aloud, instead ask the caller to repeat the information back to you to confirm).

Mail Orders

Confirm a business need with the PCI Compliance Officer. Due to security risk, Mail Orders are discouraged. Never request CVV codes on Mail Order forms and securely destroy paper records immediately after authorization. Approved designated forms must be used.

5.6 Paper Forms with Payment Card Data

Storage and Destruction

- **Approval Required:** A business need to store payment card data must be approved by the merchant department's senior management and confirmed with the PCI Compliance Officer.
- **Secure Storage:** Payment card data must be securely stored on pre-approved paper forms. Electronic storage is strictly prohibited.
- **Maintain and Inspect Inventory Logs:** Keep inventory logs of all paper records with Cardholder Data (CHD) and Card Verification Value (CVV). Inspect inventory logs at least quarterly for missing records and records that are no longer needed.
- **PCI-Compliant Destruction:** Destroy payment card data in a PCI-compliant manner—either cross-shred or dispose of in an Iron Mountain shredding box. Sensitive Authentication Data (SAD) must be destroyed immediately after authorization. Cardholder Data (CHD) must be destroyed as soon as it is no longer needed.
- **Report Missing Records:** Missing records might constitute a breach and must be reported and investigated according to the University's [Payment Card Data Security Incident Response Plan](#).

Movement, Distribution, and Transmission of Paper Forms with Payment Card Data

- **No SAD Movement/Transmission:** SAD (CVV) must never be moved, distributed, or transmitted, except by Iron Mountain for destruction.
- **Approval and Secure Transport of CHD:** Merchant management must approve moving paper records with CHD from secure storage. When sending CHD to third parties (except Iron Mountain), place data in a "Confidential" envelope and use a trusted courier. Implement procedures for logging, securing, and tracking CHD during transport.
- **Prohibit Electronic Transmission:** Payment card data must never be transmitted to or from Merchants using traditional electronic messaging technologies, including fax, email, instant messaging, SMS, etc.

5.7 Third-Party Service Providers (TPSP)

Third-Party Service Providers (TPSPs) engaged in payment solutions facilitating acceptance of credit and debit card payments by Carleton Merchants must be compliant with the latest PCI DSS. They are required to maintain their compliance throughout the duration of the agreement and provide evidence of compliance upon request and at least annually in the form of either (i) a SAQ-D for Service Providers or (ii) an Attestation of Compliance for Service Providers or (iii) a Report on Compliance.

The TPSP Onboarding Process at Carleton University includes key vetting steps and consulting with the university stakeholders such as the PCI team, ITS Security, Privacy, and Procurement. See detailed guidelines below:

TPSP Onboarding Process

Step 1	Merchant	Identify the Need for a Third-Party Solution/Platform: Prepare high-level business and functional requirements. Query ITS Service Desk for an existing solution. If a new solution is required, proceed to the next step.
Step 2	Merchant	Contact Procurement Services: Estimate the total value of the contract to determine the type of procurement and signing authority.
Step 3	Merchant	Contact Carleton Stakeholders: Engage with PCI & Business Operations, ITS Security, Privacy, and Risk and Insurance teams for preliminary requirements.
Step 4	Merchant, Procurement Services	Obtain TPSP Proposal(s): Receive and review proposals, then select a vendor.
Step 5	Merchant, ITS Security	TPSP Assessment – DPRA: Open a ticket with ITS to complete the Data Protection Risk Assessment for the selected vendor. ITS Security will share recommendations with stakeholders.
Step 6	Merchant, Procurement, Legal Team, PCI Compliance Team, Signing Authority	Contract Negotiations and Award: Ensure written agreements meet PCI requirements, including security responsibility, compliance commitment, and evidence of compliance. Finalize and sign the agreement.

Also see infographic [Appendix C: New Third-Party Service Provider Onboarding Process](#).

5.8 Annual PCI Compliance Cycle and Merchant Reporting Milestones

Merchant units must participate in the University's annual PCI compliance cycle and meet the following milestones:

January/June	Access Control: Merchants confirm that all user accounts and lists of users are up to date.
February/May/August/November	Quarterly Submissions of PIN Pad Inspection Logs: POS terminals are inspected regularly, inspections are logged, and logs submitted to the PCI Compliance Officer quarterly.
April	Incident Response Awareness: Merchants confirm their staff awareness of the University and location-specific PCI incident response plans.
May - June	Annual PCI Training: Complete annual PCI training. New staff must complete training before accessing merchant equipment and systems.

August - October	Annual PCI Merchant Questionnaires: Merchants complete their location-specific questionnaires and participate in follow-up interviews and remediation of non-compliances if required.
November - December	Internal Approvals and Report to the Industry: The PCI Steering Committee reviews compliance evidence and reports to the AVP Financial Services. If approved, the final report is submitted to Carleton's Acquiring Bank Chase Payments Canada on behalf of the payment card brands.
Other Milestones	Other milestones include submitting P2PE devices inventory and inspection logs as per the P2PE Integration Manual (PIM) schedule and monitoring TPSP's PCI DSS compliance documentation annually.

5.9 When to Proactively Contact the PCI Compliance Officer?

Merchant departments should proactively contact Carleton's PCI Compliance Officer in the following situations:

Starting or Modifying Payment Processes

- When you wish to start accepting credit/debit card payments for goods and services.
- When you wish to open or close a merchant account.
- When you wish to make changes to your existing merchant account(s) and operations, including but not limited to:
 - Choosing a new third-party service provider.
 - Changing your approved e-commerce integration model (e.g., upgrading from redirect to iFrame or API).
 - Modifying the approved method of accepting credit/debit card payments (e.g., adding the Telephone Order stream, identifying the business need to store CHD, etc.).
 - Adding a new VoIP extension to the department's Telephone Order Extension Inventory.
 - Changing the number and type of POS terminals in your possession.
 - Moving your POS terminal(s) to a different location (including off-site).
 - Identifying the need to temporarily store payment card data.

Equipment and Training

- When your POS terminal has been replaced by an authorized technician due to a failure.
- When a new PCI training need has been identified.

Security Incidents

- When you suspect a security incident, as per the [University's Payment Card Data Security Incident Response Plan](#).

6. References

[1] PCI SSC Glossary: <https://www.pcisecuritystandards.org/glossary/>

[2] Validated Payment Software:

https://listings.pcisecuritystandards.org/assessors_and_solutions/payment_software?agree=true

[3] Approved PTS Devices:

https://listings.pcisecuritystandards.org/assessors_and_solutions/pin_transaction_devices?agree=true

[4] PCI P2PE Solutions:

https://listings.pcisecuritystandards.org/assessors_and_solutions/point_to_point_encryption_solutions?agree=true

7. Glossary

[A](#) [B](#) [C](#) [D](#) [E](#) [F](#) [G](#) [H](#) [I](#) [J](#) [K](#) [L](#) [M](#) [N](#) [O](#) [P](#) [Q](#) [R](#) [S](#) [T](#) [U](#) [V](#) [W](#) [X](#) [Y](#) [Z](#)

A

Access Control – the process of managing user access to PCI terminals and systems, e.g., enabling/disabling user accounts and granting permissions based on the [Business Need to Know](#).

Acquiring Bank – also known as “acquirer”, “processing bank” or “merchant bank”. An entity, typically a financial institution, that provides all payment card processing services, including settlement into the merchant’s account, and is defined by payment brands as an acquirer [1].

Application (e-commerce) – in the context of this document, a software program, e.g., a web application or a “store front”, created in-house or by a third-party, hosted on-premises or in the cloud (SaaS). The application owner (internal or third-party) is responsible for integrating with a payment gateway and the merchant’s account with the University’s acquiring bank.

Application Vendor (e-commerce) – an external (third-party) owner of the application software.

Approved POS Terminal – A cellular, wired, or P2PE POS terminal provided either by the university’s Acquiring Bank or by a third-party service provider vetted through the [New Third-Party Service Provider Onboarding Process](#).

Attestation of Compliance (AOC) - The AOC is a form for merchants and service providers to attest to the results of a PCI DSS assessment, as documented in the Self-Assessment Questionnaire or Report on Compliance. [1]

Authentication – Process of verifying identity of an individual, device, or process. Authentication typically occurs through the use of one or more authentication factors such as:

- Something you know, such as a password or passphrase
- Something you have, such as a token device or smart card
- Something you are, such as a biometric. [1]

Authorization - In the context of access control, authorization is the granting of access or other rights to a user, program, or process. Authorization defines what an individual or program can do after successful authentication. In the context of a payment card transaction, authorization refers to the authorization process, which completes when a merchant receives a transaction response (for example, an approval, decline, or an error message) from the issuing bank. [1]

B

Business Need to Know is defined here as (a) access to the payment card data/environment limited to as few people as possible and (b) level of access to the cardholder data/environment is set as the least necessary to perform assigned responsibilities.

C

Card not Present (CNP) Transaction – a transaction completed without card present via e-commerce, over the phone (Telephone Order, TO), or by mail (Mail Order, MO). For e-commerce, transactions are initiated

and completed by the cardholder. For Telephone and Mail Orders, transactions are initiated and completed by the merchant.

Card Present (CP) Transaction – a face-to-face transaction, initiated by the merchant and completed by the cardholder.

Card Verification Code - Also referred to as Card Validation Code or Value, or Card Security Code. For PCI DSS purposes, it is the three- or four-digit value printed on the front or back of a payment card. May be referred to as CAV2, CVC2, CVN2, CVV2, or CID according to the individual Participating Payment Brands. For more information, contact the Participating Payment Brands. [1]

Cardholder Data (CHD) – Cardholder data includes the full Primary Account Number (PAN) plus any of the following: cardholder name, expiration date and/or service code. [1] See [Sensitive Authentication Data](#) for additional data elements that may be transmitted or processed (but not stored) as part of a payment transaction.

Cardholder Data Environment (CDE) - the people, processes and technology that store, process, or transmit Cardholder Data or [Sensitive Authentication Data](#). [1]

Carleton Merchant – Carleton department that accepts credit/debit cards as payment for goods and/or services and has an approved merchant account (MID) with the University's Acquiring Bank Chase Payments Canada.

D

Data Breach – A confirmed [security incident](#) that results in the loss of personal data, including payment card data.

[Data Protection and Risk Assessment \(DPRA\)](#) - A process involving ITS's Service Delivery & Quality group, Information Security group, and Privacy Office to evaluate security and privacy risks of an IT system or service. The DPRA report identifies risks, assigns a risk level score, and provides recommendations to mitigate significant risks. This helps merchant departments make informed decisions to protect users and the university.

E

Electronic Commerce - commonly known as e-commerce and consists of the buying and selling of products or services over electronic systems such as the internet; transactions are initiated by cardholders in their browsers.

F

Fully Hosted Solution – a solution that is outsourced to a third-party service provider(s); both, Application and Gateway, are fully hosted off-site (in cloud) on service providers' servers; service providers are fully responsible for the security of CHD.

G

H

I

Issuing Bank - Also referred to as "issuer" or "issuing financial institution". Entity that issues payment cards

or performs, facilitates, or supports issuing services including but not limited to issuing banks and issuing processors. [1]

J

K

L

Long-term – on regular basis for a period of over a year.

M

MAC Address – Abbreviation for “media access control address” [1]. These are unique identifying values assigned by manufacturers to wired POS terminals. These values are used to monitor authorized traffic on Carleton’s [PCI network](#).

Mail Order, MO – payment information mailed on a designated paper form (must exclude CVV) and manually keyed into the POS terminal as a ‘mail order’ by merchant staff to complete the sale.

Merchant - For the purposes of the PCI DSS, a merchant is defined as any entity that accepts payment cards bearing the logos of any PCI SSC Participating Payment Brand (American Express, Discover, JCB, Mastercard, or Visa) as payment for goods and/or services. [1]

Merchant Account – account with the Acquiring Bank for settling proceeds from credit/debit card sales.

Merchant of Record – an entity that holds a Merchant Account, either at Carleton or through a third-party. Carleton departments typically manage their merchant accounts and ensure PCI compliance. When wholly outsourced, the service provider becomes the merchant of record, handling PCI-compliant credit/debit card payments for Carleton University. The provider’s name appears on receipts, and proceeds are forwarded to the University’s department as agreed.

Method of Payment (MOP) – In the context of this manual, these are types of payment cards a merchant wishes to accept, e.g., Visa, Mastercard, Visa Debit, Debit Mastercard, Interac, American Express.

N

O

P

Payment (Card) Brand – Payment industry entities responsible for facilitating payment card transactions as well as setting operating rules and compliance requirements. Visa, Mastercard, American Express, Discover, and JCB International are founding members of the [PCI SSC](#).

Payment Card – a credit or debit card issued by one of the leading card brands, e.g., Visa, Mastercard, or American Express, and bearing their logo. [1]

Payment Card Data - Also known as “account data”, consists of [Cardholder Data](#) and [Sensitive Authentication Data](#).

Payment Gateway – The service that automates the payment transaction between the merchant and a customer. It is usually a third-party service that processes, verifies, and accepts or declines card transactions on behalf of the merchant, via secure internet connections.

Payment Software - A software that stores, processes, or transmits payment card data as part of authorization or settlement [1]. Also see [Validated Payment Software](#).

Payment Stream – Also referred to as “payment channel”. Dependent on how Carleton merchants process payment card data, they qualify for one of the following payment streams approved at Carleton:

A	e-commerce, no CHD and SAD on merchant’s servers, all payment processing is outsourced to PCI DSS compliant third-party service providers (TPSP)
B	all payment processing is via PCI-listed [3] cellular stand-alone POS terminals
B-IP	all payment processing is via PCI-listed [3] wired stand-alone POS terminals connected to Carleton’s secure PCI network
P2PE	all payment processing is via POS terminals from a validated PCI-listed Point-To-Point Encryption solution [4]
C-VT	all payment processing is via CU ITS-validated device and a virtual payment terminal solution provided and hosted by a PCI DSS compliant third-party service provider (TPSP)

PCI DSS - The Payment Card Industry (PCI) Data Security Standard (DSS) aims to improve payment card data security by promoting the adoption of consistent security measures worldwide. PCI DSS outlines technical and operational requirements to protect payment card data and can also help secure other elements in the payment ecosystem. [1]

PCI Network – A secure, segregated network dedicated to payment card data traffic only. Carleton’s PCI network is set up and maintained by [ITS Network Services](#) and enables payment streams B-IP and C-VT.

PCI SSC – The Payment Card Industry (PCI) Security Standard Council (SSC) is an open global forum established in 2006. It aims to enhance payment security by developing and managing Global Payment Security Standards, validating payment solutions, training PCI professionals, and promoting awareness through free educational resources for the PCI community.

POS Terminal – a point-of-sale terminal used for processing in-person (Card Present, CP) and over-the-phone (Card-not-Present Telephone Order, CNP TO) payments.

Primary Account Number (PAN) - Also referred to as “account number.” Unique payment card number (typically for credit or debit cards) that identifies the issuer and the particular cardholder account. [1]

Q

Qualified Security Assessor (QSA) - QSAs are qualified by PCI SSC to perform PCI DSS on-site assessments. Refer to the QSA Qualification Requirements for details about requirements for QSA Companies and Employees. [1]

R

S

SAQ - Acronym for “Self-Assessment Questionnaire.” Reporting tool used to document self-assessment

results from an entity's PCI DSS assessment. [1]

Security Incident – An occurrence considered by an organization to have potential security implications to a system or its environment. In the context of PCI DSS, security events identify suspicious or anomalous activity. [1]

Sensitive Authentication Data (SAD) - security-related information (including but not limited to card validation codes/values, full track data (from the magnetic stripe or equivalent on a chip), PINs, and PIN blocks) used to authenticate cardholders and/or authorize payment card transactions. [1]

Short-term – one-time, on occasional basis or for a period of less than a year.

Supporting documentation – Includes receipts, invoices, and other records containing partial card numbers. Merchants must retain these documents for seven years as required by Canada Revenue Agency.

T

Telephone Order, TO - payment information communicated to the merchant staff over the phone (must include CVV) and manually keyed into the POS terminal as a 'telephone order' by merchant staff to complete the sale.

Third-Party Service Provider (TPSP) – also known as "service provider" or "vendor". An entity that is not a payment brand, directly involved in the processing, storage, or transmission of payment card data on behalf of a merchant. This also includes companies that provide services that control or could impact the security of payment card data. Examples include hosting providers. [1]

U

V

Validated Payment Software – Payment software assessed by a Secure Software Assessor to confirm adherence to the PCI Secure Software Standard. [2]

Virtual Payment Terminal (Virtual Terminal, VT) - A virtual payment terminal uses a web browser to access an acquirer, processor, or third-party service provider's site for authorizing card transactions. The merchant manually inputs card data through a secure web connection. Unlike physical terminals, virtual terminals don't read card data; staff enter transactions manually via a **Virtual Terminal Device** [1]. An e-commerce merchant account and a dedicated VT device are required for this option.

Virtual Terminal Device – a PCI DSS compliant computer/cellular device, dedicated solely to manually entering transactions directly to the card processing company's website (gateway). The device must be vetted by the university's ITS Security.

W

X

Y

Z

Appendix A: Opening a Merchant Account with the Approved Acquirer

To set up a merchant account with the approved acquirer, follow these steps:

Step 1	Merchant	Identify Requirements: Prepare high-level business and functional requirements.
Step 2	Merchant	Identify Resource Needs: Determine the need for in-house ITS and Project Management resources and submit an ITS ticket if necessary. If a Third-Party Service Provider (TPSP) is required, proceed to the next step.
Step 3 TPSP	Merchant	<p>Additional Step to Onboard a Third-Party Service Provider (TPSP) Appendix C: New Third-Party Service Provider Onboarding Process</p> <p>Onboard a TPSP: Review relevant policies and procedures, and contact University stakeholders for guidance.</p>
Step 4	Merchant, Financial Services	Financial Infrastructure: Contact Financial Services early for information about index/FOAPAL and fund advice.
Step 5	Merchant	Refund Policy: Document the department's refund policy.
Step 5	Merchant, PCI Compliance Officer	Merchant Account Consultation: Consult with the PCI Compliance Officer to determine merchant type, equipment, systems, operating costs, and PCI requirements.
Step 6	Merchant	Merchant Account Request: Provide necessary information to the PCI Compliance Officer, including merchant name, address, product/service description, equipment required, estimated annual transaction volumes by the card type, and an average transaction size.
Step 7	Merchant	Identify Merchant Contacts: Assign Merchant Management, Operations, and Technical Leads, and inform the PCI Compliance Officer.
Step 8 E-commerce	Merchant, Developer	<p>Additional Step for E-Commerce Merchants Only Appendix D: New E-commerce Merchant Location Approval Process</p> <p>Develop and Test in Demo Environment: Ensure the payment solution operates as intended in a pre-production environment and complies with the following 12 receipt requirements:</p> <ol style="list-style-type: none"> 1. The date the processing data for the relevant Internet Transaction was obtained. 2. Your business trade name and website address. 3. The card type used in the Internet Transaction (DO NOT INCLUDE THE FULL PAN; last four digits are allowed: xxxxxxxxxx1234). 4. The amount and type (purchase or credit) of the applicable Internet Transaction. 5. The currency in which the transaction was processed (CDN or CAD).

		<ol style="list-style-type: none"> 6. The authorization number assigned to the Internet Transaction by the Issuing Bank. 7. The unique Internet Transaction order number assigned by you/your application. 8. A detailed description of the Internet Transaction goods or services. 9. The contact name, mailing address, email address, telephone, and fax number of a person representing you for Internet Transaction disputes. 10. Applicable Merchant taxation or export information (Carleton's HST number). 11. The name of the purchaser of your goods or services. 12. Return/refund policy. <p>Development Guidelines</p> <ul style="list-style-type: none"> • Test Card Numbers: Use test card numbers for testing in pre-production environment. • URL Redirect: Use URL redirect for all e-commerce applications hosted on Carleton's servers. iFrame and API integrations are not permitted for in-house developments. • Collaboration: Website development should be carried out in collaboration with the University's ITS Security and the PCI Compliance Officer to effectively mitigate information technology risks and ensure PCI Compliance.
Step 9 Virtual Terminal	Merchant, ITS Security	<p>Additional Step for Virtual Terminal Merchants Only</p> <p>Appendix E: Deployment and Physical Security of a Virtual Terminal Device</p> <p>Virtual Terminal Setup: Purchase and configure the Virtual Terminal Device as per ITS Security's specifications.</p>
Step 10 Wired POS Devices	Merchant, ITS	<p>Additional Step for Merchants with Wired POS Terminals and Virtual Terminal Devices</p> <p>Wired POS Devices Setup: Request PCI Network Port(s) and ensure that they're located in areas not accessible to public.</p>
Step 11	Merchant	Complete New Merchant Documentation: Fill out the New Merchant Onboarding Questionnaire, create an Incident Response Plan, and document Merchant Operational Procedures.
Step 12	Merchant	Mandatory PCI Training: Ensure all merchant team members complete PCI training.
Step 13	PCI Compliance Officer	Apply for Merchant ID: The PCI Compliance Officer will submit the request to the Acquirer and seek approval of the AVP Financial Services.
Step 14	Merchant	Organize Financial Reporting: Contact the Receipt Accounting team for financial reconciliation and reporting.

Step 15 POS Terminals	Merchant	Additional Step for Merchants with POS Terminals Onboard New POS Terminals: Ensure secure storage of terminals, record serial numbers and locations of terminals, and set up unique accounts for users with void/refund privileges.
Step 16 E-commerce	Merchant, PCI Compliance Officer	Additional Step for E-commerce Merchant Accounts E-commerce Platform Access: Set up unique user accounts and grant access based on business-need .
Step 17 E-commerce	Merchant, Developer	Additional Step for E-commerce Merchant Accounts Develop and Test in Production Environment: Ensure the payment solution operates as intended in production environment and complies with the following 12 receipt requirements: <ol style="list-style-type: none"> 1. The date the processing data for the relevant Internet Transaction was obtained. 2. Your business trade name and website address. 3. The card type used in the Internet Transaction (DO NOT INCLUDE THE FULL PAN; last four digits are allowed: xxxxxxxxxxx1234). 4. The amount and type (purchase or credit) of the applicable Internet Transaction. 5. The currency in which the transaction was processed (CDN or CAD). 6. The authorization number assigned to the Internet Transaction by the Issuing Bank. 7. The unique Internet Transaction order number assigned by you/your application. 8. A detailed description of the Internet Transaction goods or services. 9. The contact name, mailing address, email address, telephone, and fax number of a person representing you for Internet Transaction disputes. 10. Applicable Merchant taxation or export information (Carleton's HST number). 11. The name of the purchaser of your goods or services. 12. Return/refund policy.
Step 18 E-commerce	Merchant, PCI Compliance Officer	Additional Step for E-commerce Merchant Accounts Final Approval for E-commerce Merchants: Obtain final approval from the AVP Financial Services before going live.
Step 19	Merchant	Begin accepting payment cards and compliance reporting .
Step 20	Business Operations	Schedule Merchant orientation sessions with Receipt Accounting and PCI Compliance Officer.

Appendix B: Closing a Merchant Account

To close a Merchant Account, follow these steps:

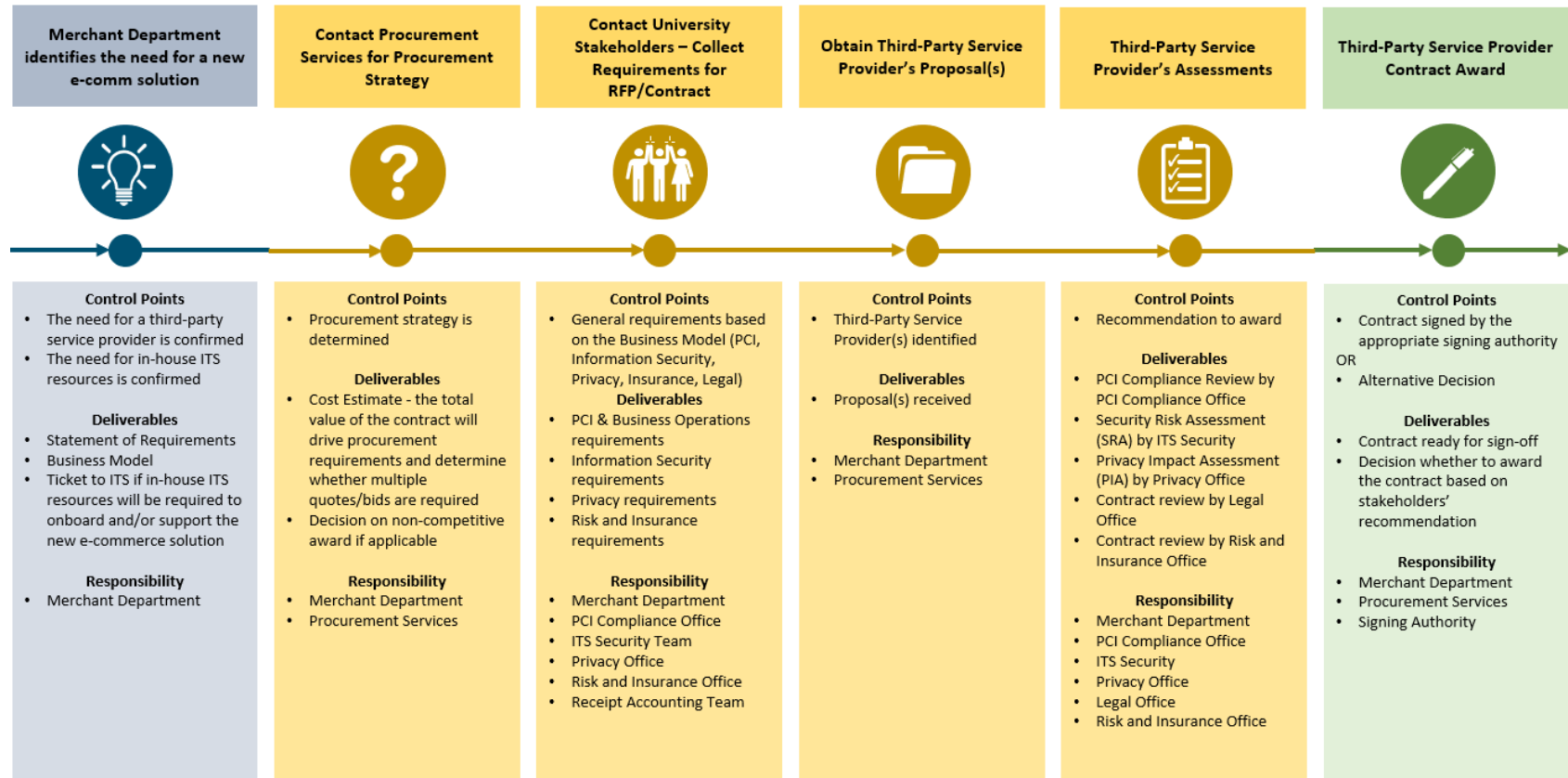
Step 1	Merchant	Request to Close Merchant Account: Email the PCI Compliance Officer with a request to close the merchant account.
Step 2 POS Terminals	Merchant, PCI Compliance Officer	<p>Additional Step for Merchants with POS Terminals</p> <p>Decommission POS Terminals</p> <ul style="list-style-type: none"> • Settle POS Terminals: Merchants must settle their POS terminals before closing the account and disposing of the equipment. • Return Equipment <ul style="list-style-type: none"> ◦ The PCI Compliance Officer facilitates the return of the Acquirer's equipment. ◦ Units that own their POS terminals or rent from a third-party other than the University's Acquirer must follow their TPSP's instructions for safe disposal of the equipment. ◦ P2PE merchants must adhere to their TPSP's P2PE Instruction Manual (PIM) for handling redundant terminals.
Step 3 E-Commerce VT Portal	Merchant	<p>Additional Step for E-Commerce or Virtual Terminal Merchants</p> <p>Decommission E-commerce and Virtual Terminal Portal</p> <ul style="list-style-type: none"> • Remove Public Access and Delete Data: Remove public access to the URL (for e-commerce), delete payment pages and recurring portfolios. • Disable User Accounts: Disable all user accounts on the merchant's gateway and/or virtual terminal portals. • Shut Down Gateway/Virtual Terminal Accounts: <ul style="list-style-type: none"> ◦ The PCI Compliance Officer will assist with decommissioning the Acquirer's gateway. ◦ Merchants using other gateways and/or virtual terminal portals must follow up with their TPSPs directly. • Access to the Virtual Terminal Device: Email a request to the PCI Compliance Officer to disable access to the virtual terminal device and provide the list of users.
Step 4	PCI Compliance Officer	Request Account Closure: Email the Acquirer to close the merchant account and discontinue billing.

Step 5 Wired POS Devices	Merchant	Additional Step for Merchants with Wired POS Terminals and Virtual Terminal Devices Confirm PCI Network Port Location Information: Email to the PCI Compliance Officer the Building Number, Room Number, and Jack Number.
Step 6 Wired POS Devices	PCI Compliance Officer	Additional Step for Merchants with Wired POS Terminals and Virtual Terminal Devices Decommission Access to PCI Network: The PCI Compliance Officer will contact Network Services to decommission dedicated PCI network ports.

Appendix C: New Third-Party Service Provider Onboarding Process

New Third-Party Service Provider Onboarding Process

In accordance with Carleton's Cash/Cash Equivalent Handling, Procurement, and Data Protection and Risk Management [Policies](#)



New Third-Party Service Provider Onboarding Process

In accordance with Carleton's Cash/Cash Equivalent Handling, Procurement, and Data Protection and Risk Management [Policies](#).

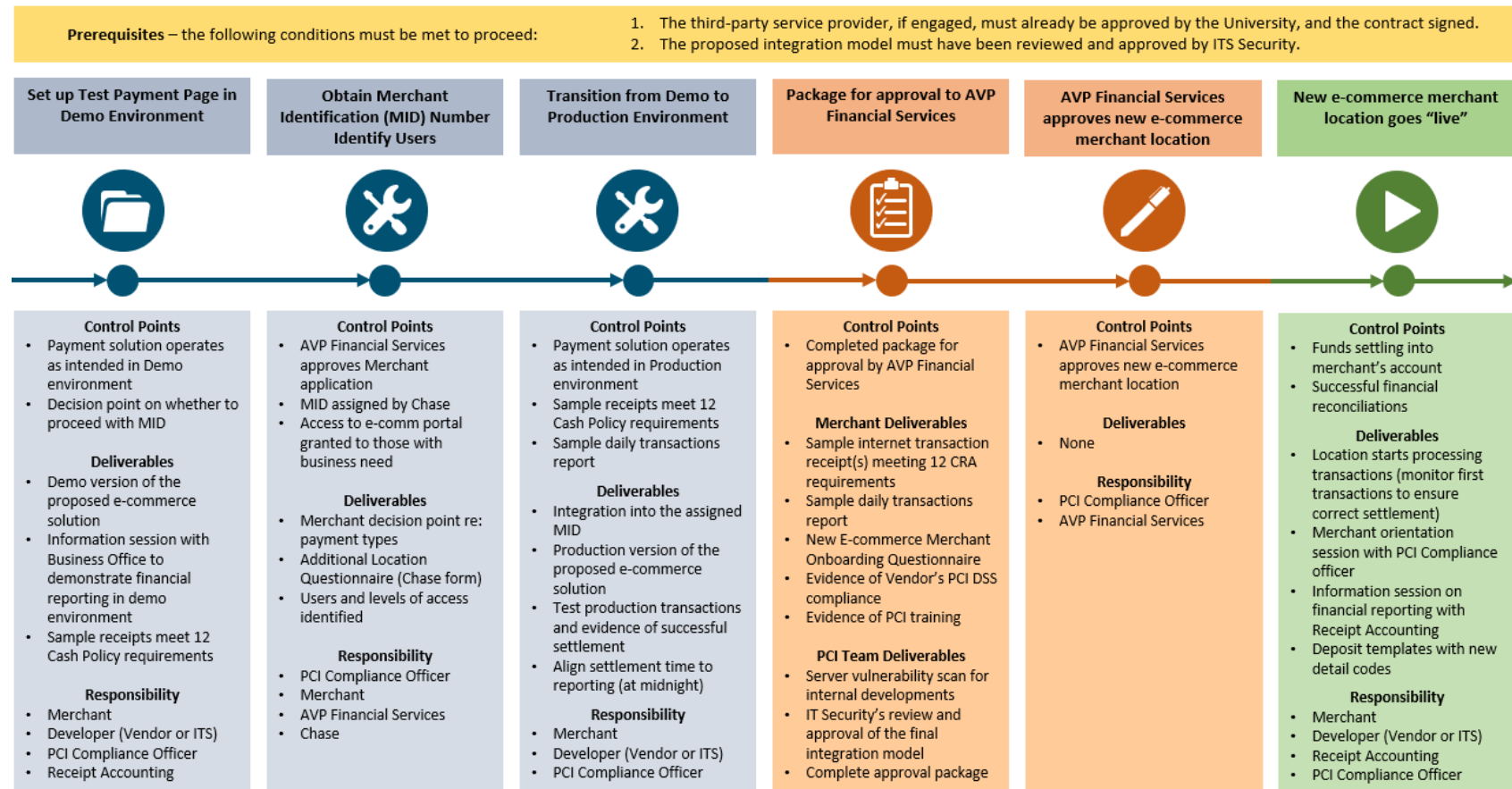
Step 1	Merchant	Merchant Department identifies the need for a new e-comm solution Control Points: <ul style="list-style-type: none"> • The need for a third-party service provider is confirmed • The need for in-house ITS resources is confirmed Deliverables: <ul style="list-style-type: none"> • Statement of Requirements • Business Model • Ticket to ITS if in-house ITS resources will be required to onboard and/or support the new e-commerce solution
Step 2	Merchant, Procurement Services	Contact Procurement Services for Procurement Strategy Control Points: <ul style="list-style-type: none"> • Procurement strategy is determined Deliverables: <ul style="list-style-type: none"> • Cost Estimate - the total value of the contract will drive procurement requirements and determine whether multiple quotes/bids are required • Decision on non-competitive award if applicable
Step 3	Merchant, PCI Compliance Officer, ITS Security, Legal & Risk, Receipt Accounting	Contact University Stakeholders – Collect Requirements for RFP/Contract Control Points: <ul style="list-style-type: none"> • General requirements based on the Business Model (PCI, Information Security, Privacy, Insurance, Legal) Deliverables: <ul style="list-style-type: none"> • PCI & Business Operations requirements • Information Security requirements • Privacy requirements • Risk and Insurance requirements
Step 4	Merchant, Procurement Services	Obtain Third-Party Service Provider's Proposal(s) Control Points: <ul style="list-style-type: none"> • Third-Party Service Provider(s) identified Deliverables: <ul style="list-style-type: none"> • Proposal(s) received

Step 5	Merchant, PCI Compliance Officer, ITS Security, Legal & Risk	Third-Party Service Provider's Assessments Control Points: <ul style="list-style-type: none"> • Recommendation to award Deliverables: <ul style="list-style-type: none"> • PCI Compliance Review by PCI Compliance Office • Security Risk Assessment (SRA) by ITS Security • Privacy Impact Assessment (PIA) by Privacy Office • Contract review by Legal Office • Contract review by Risk and Insurance Office
Step 6	Merchant, Procurement Services, Signing Authority	Third-Party Service Provider Contract Award Control Points: <ul style="list-style-type: none"> • Contract signed by the appropriate signing authority OR <ul style="list-style-type: none"> • Alternative Decision Deliverables: <ul style="list-style-type: none"> • Contract ready for sign-off • Decision whether to award the contract based on stakeholders' recommendation

Appendix D: New E-commerce Merchant Location Approval Process

New E-commerce Merchant Location Approval Process

In accordance with Carleton's [Cash/Cash Equivalent Handling Policy](#)



New E-commerce Merchant Location Approval Process

In accordance with Carleton's [Cash/Cash Equivalent Handling Policy](#).

Prerequisites – the following conditions must be met to proceed:

1. The third-party service provider, if engaged, must already be approved by the University, and the contract signed.
2. The proposed integration model must have been reviewed and approved by ITS Security.

Step 1	Merchant, Developer (Vendor or ITS), PCI Compliance Officer, Receipt Accounting	Set up Test Payment Page in Demo Environment Control Points: <ul style="list-style-type: none"> • Payment solution operates as intended in Demo environment • Decision point on whether to proceed with MID Deliverables: <ul style="list-style-type: none"> • Demo version of the proposed e-commerce solution • Information session with Business Office to demonstrate financial reporting in demo environment • Sample receipts meet 12 Cash Policy requirements
Step 2	PCI Compliance Officer, Merchant, AVP Financial Services, Acquirer (Chase)	Obtain Merchant Identification (MID) Number; Identify Users Control Points: <ul style="list-style-type: none"> • AVP Financial Services approves Merchant application • MID assigned by Chase • Access to e-comm portal granted to those with business need Deliverables: <ul style="list-style-type: none"> • Merchant decision point re: payment types • Additional Location Questionnaire (Chase form) • Users and levels of access identified
Step 3	Merchant, Developer (Vendor or ITS), PCI Compliance Officer	Transition from Demo to Production Environment Control Points: <ul style="list-style-type: none"> • Payment solution operates as intended in Production environment • Sample receipts meet 12 Cash Policy requirements • Sample daily transactions report Deliverables: <ul style="list-style-type: none"> • Integration into the assigned MID • Production version of the proposed e-commerce solution • Test production transactions and evidence of successful settlement • Align settlement time to reporting (at midnight)

Step 4	Merchant, PCI Compliance Team	Package for approval to AVP Financial Services Control Points: <ul style="list-style-type: none"> Completed package for approval by AVP Financial Services Merchant Deliverables: <ul style="list-style-type: none"> Sample internet transaction receipt(s) meeting 12 CRA requirements Sample daily transactions report New E-commerce Merchant Onboarding Questionnaire Evidence of Vendor's PCI DSS compliance Evidence of PCI training PCI Team Deliverables: <ul style="list-style-type: none"> Server vulnerability scan for internal developments IT Security's review and approval of the final integration model Complete approval package
Step 5	PCI Compliance Officer, AVP Financial Services	AVP Financial Services approves new e-commerce merchant location Control Points: <ul style="list-style-type: none"> AVP Financial Services approves new e-commerce merchant location Deliverables: <ul style="list-style-type: none"> None
Step 6	Merchant, Developer (Vendor or ITS), Receipt Accounting, PCI Compliance Officer	New e-commerce merchant location goes "live" Control Points: <ul style="list-style-type: none"> Funds settling into merchant's account Successful financial reconciliations Deliverables: <ul style="list-style-type: none"> Location starts processing transactions (monitor first transactions to ensure correct settlement) Merchant orientation session with PCI Compliance officer Information session on financial reporting with Receipt Accounting Deposit templates with new detail codes

Appendix E: Deployment and Physical Security of a Virtual Terminal Device

Virtual Terminal (VT) device is a PCI DSS compliant computer device, dedicated solely to entering transactions directly to the card processing company's website (gateway). When employing such device, the following requirements must be followed:

- A dedicated, single-purpose workstation must be used.
- Only devices pre-approved and pre-configured by ITS Security must be used. For information and assistance, please contact ITS.Security@cunet.carleton.ca. ITS Security will ensure compliance with the following requirements:
 - ✓ Automated patching
 - ✓ Restrictive firewalling
 - ✓ PCI compliant antivirus solution
 - ✓ Removal of any unnecessary software/services
 - ✓ Disabled USB
 - ✓ Remote access disabled
 - ✓ Appropriate logging
- Virtual Terminal devices must be connected to Carleton's PCI network - a segmented VLAN logically separated from the rest of the network. Each virtual terminal device will be assigned a unique private IP address. For assistance with an existing jack or to install a new dedicated PCI network jack, please contact ITSServiceDesk@Cunet.Carleton.Ca. Ensure you indicate that you require access to Carleton's PCI network.
- Virtual Terminal devices must be physically secured and not located in publicly accessible areas:
 - ✓ When not in use, disconnect the network cable from your VT device and store the device securely;
 - ✓ Restrict access to the virtual POS and the VT device by business need;
 - ✓ Control access to the VT terminal(s) and equipment; verify credentials prior to granting access (e.g., repair personnel);
 - ✓ Escort authorized personnel during repairs/ maintenance;
 - ✓ Prevent unauthorized individuals from accessing VT terminal(s) and equipment;
 - ✓ Always log out to prevent unauthorized access to payment card data;
 - ✓ Regularly inspect VT device(s) and report any suspicious activity (e.g., a new wire/cables attached to the device) immediately as per [Carleton's Payment Card Data Security Incident Response Plan](#);
 - ✓ Never leave a VT terminal unlocked or unattended.
- A current list of users requiring access to each device must be communicated to PCICompliance@Carleton.Ca. The Department must notify PCICompliance@Carleton.Ca of any changes to the list, so access profiles can be updated accordingly.
- Unique user accounts must be configured with passwords in adherence to the [University Information Technology \(IT\) Security Policy](#).
- No electronic storage of payment card data is permitted.

Appendix F: Point of Sale Terminal Security Training and Procedures

POS terminal security focuses on protecting POS devices. Merchants must safeguard their payment systems and infrastructures to prevent POS fraud. They must implement controls required by the PCI DSS.

Key tasks include:

- Training staff on POS device security, including to verify identity of repair technicians and accompany them during their work.
- Limiting access to POS terminals by business need.
- Keeping a list of users and their access privileges.
- Maintaining an inventory of POS devices.
- Performing regular inspections to detect any compromise early.
- Recording inspections in designated PIN Pad Inspection Logs.
- Submitting inspection logs quarterly to the PCI Compliance Officer.
- Recognising signs and responding promptly to any security breaches.

Schedule of Quarterly Submissions:

Quarter	Months	Submission
1	May-July	August
2	August-October	November
3	November-January	February
4	February-April	May

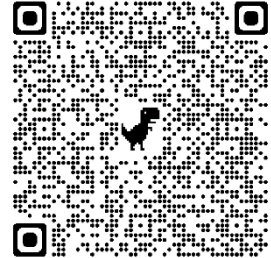
Inspection Process:

- Check for illegal equipment like skimmers or cameras.
- Ensure serial numbers match your records.
- Look for signs of tampering (e.g., broken/replaced parts, loose keypad, unusual wires, signs of device being opened).
- If the terminal flashes “Irruption!”, contact the Acquirer helpdesk immediately.
- Initiate the Incident Response Plan if fraud is suspected.
- Use the approved PIN Pad Inspection Log template to log your inspections.

Appendix G: Payment Card Data Security Incident Response Plan: Standalone Cellular & Wired Terminals












Business Name: _____
Incident Response Lead: _____
Incident Response Deputy: _____
Manager/Director to Notify: _____



THREAT INDICATORS

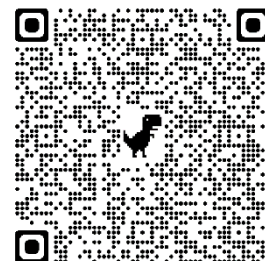
- Signs of break-in/damage on a secured, locked cabinet storing payment card data;
- Lost paper forms containing payment card data;
- A skimming device or unusual attachment on a POS device;
- A tamper warning message or a broken tamper proof seal on a POS device;
- Serial numbers on the PIN pad device not matching those on record, indicating a switch;
- A missing POS device, indicating theft or loss;
- Unfamiliar equipment near your PCI terminal or POS device;
- Hidden camera recording entry of authentication credentials;
- Multiple refunds going to the same card;
- Customer reports compromised credit/debit card;
- Suspicious behaviour around devices

-  **STOP** processing transactions immediately
-  DO NOT unplug power
-  If IP-connected - **unplug network cable**
-  DO NOT alter or access the compromised system (e.g., do not log in to change passwords)
-  Preserve logs and electronic evidence
-  Notify your supervisor and the designated incident response lead/deputy
-  Call **613-520-3700** and email ITSServiceDesk@cunet.carleton.ca to report the incident indicating **urgency, PCI & credit card breach**
-  Notify PCICompliance@Carleton.ca
-  Log all actions taken

Appendix H: Payment Card Data Security Incident Response Plan: E-Commerce & Virtual Terminal



Business Name: _____
Incident Response Lead: _____
Incident Response Deputy: _____
Manager/Director to Notify: _____



THREAT INDICATORS

E-Commerce

A third-party partner reports a breach
Suspicious financial transactions
Suspicious activity on the Application
Unauthorized access to a system or network
Gateway and application's daily financial reports don't reconcile

Virtual Terminal and Gateway Access

Suspected malware:

- Frequent random pop-up windows
- Passwords no longer working
- Anti-virus alerts or anti-virus shutting down
- Frequent crashes or unusually slow performance
- Hung process

Customer reports compromised credit/debit card
Hidden camera recording entry of credentials



STOP processing transactions immediately



DO NOT unplug power



If Virtual Terminal - **unplug network cable**



DO NOT alter or access the compromised system (e.g., do not log in to change passwords)



Preserve electronic evidence



Notify your supervisor and the designated incident response lead/delegate



Call **613-520-3700** and email ITSServiceDesk@cunet.carleton.ca to report the incident indicating **urgency, PCI & credit card breach**



Notify PCCompliance@Carleton.ca



Log all actions taken