# PAYMENT CARD ACCEPTANCE PROCEDURES

Contact Officer PCI Coordinator

## Purpose

The purpose of these procedures is to outline the steps that departments, faculties, and units (“merchants”) must follow for all payment card (debit and credit card) transactions at Queen’s University. All merchants that accept payment cards must follow these procedures for the protection of payment card data as described in the Payment Card Industry Data Security Standards (PCI DSS), and as further contained in the University’s Payment Card Acceptance Policy.

## Contents

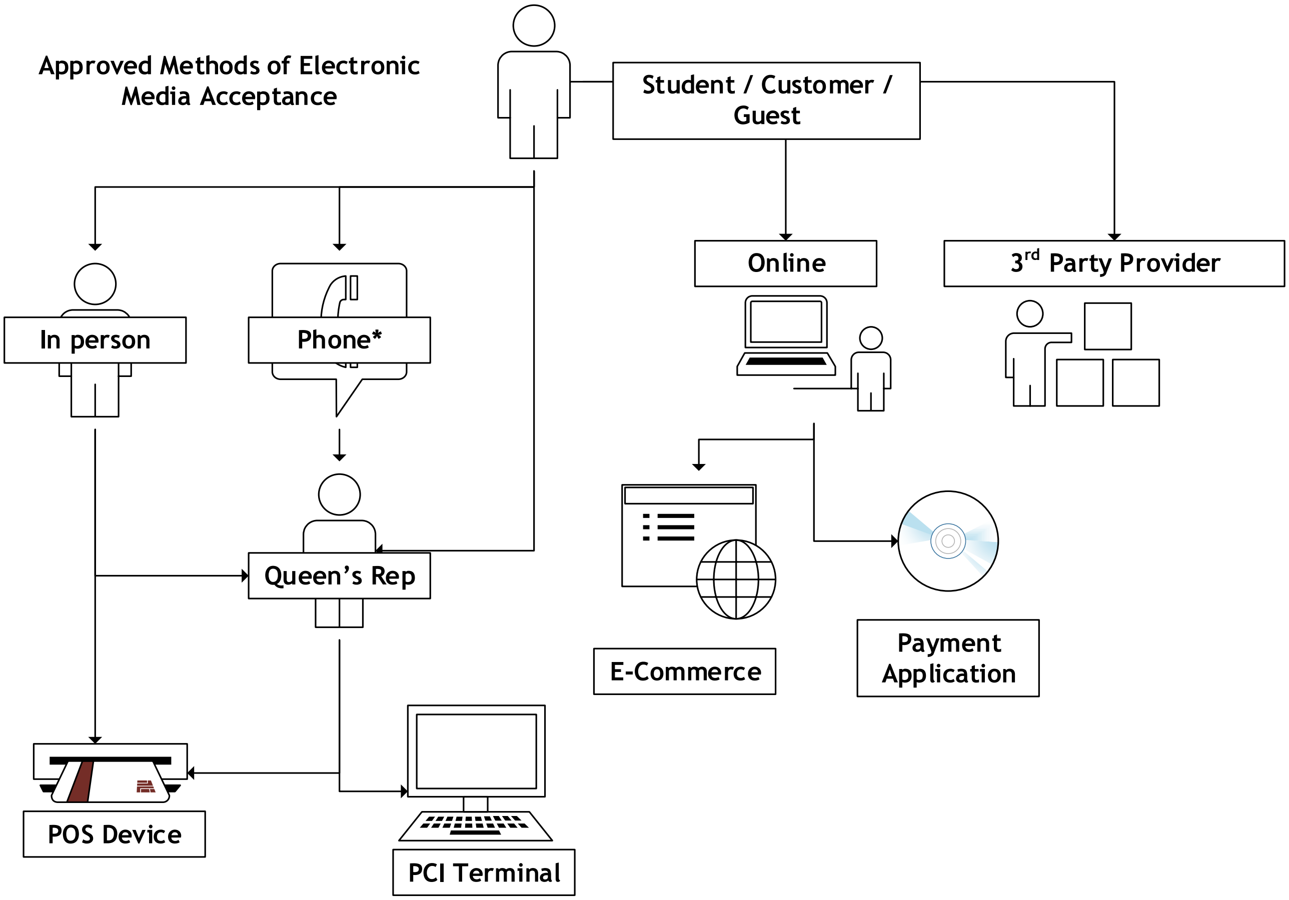
# *Procedure*

## 1.0 Approved Methods for Accepting, Storing, and Disposing of Payment Card Data

### 1.1 Accepting Electronic Media

Merchants are able to accept payment card data electronically if it is received in any of the following ways:

- In person:
  - Where the customer enters their data directly into a PCI PTS compliant and Queen's approved POS device (either purchased by the merchant or leased from the acquirer).
  - Where either the customer enters their data through a PCI PTS compliant POS device, or a trained Queen's representative enters the data into the payment application or approved payment gateway via a PCI terminal.
- Phone:
  - Where the customer provides their information to a trained Queen's representative who processes it immediately using either a PCI terminal or a PCI PTS compliant POS device.
- Online:
  - Where the customer enters their payment card data directly into the e-commerce payment gateway.
  - Where the customer enters their payment card data directly into a payment gateway as part of a P2PE solution or PA DSS certified payment application.
- 3rd Party Service Provider
  - Where the customer enters their payment card data directly into the service provider's payment gateway.



*If telephone processing involves technologies such as VOIP, wireless headsets, etc., it needs to be approved by the PCI Coordinator prior to use.

Merchants must ensure the security of electronic media. Remember to log off when away from them. If using a PCI terminal, log out as soon as transactions have been completed.

## 1.2 Approved Methods of Electronic Media Storage

Payment card data is NEVER to be stored locally in any form. It should never be stored on Queen's internal or external hard drives, solid state or USB "flash" drives, memory cards, smartphones, tablets, CDs, DVDs, or Blu-ray discs.

Any merchant using a POS device must ensure that it is stored in a secure and locked location when not in use.

Approved acquirers, payment applications, and/or service providers may store payment card data on behalf of Queen's. It must be encrypted, masked, or truncated. Acquirers, payment applications, and/or service providers storing data on behalf of Queen's must adhere to the PCI DSS and have signed a contract indemnifying Queen's for all costs related to a potential or actual security breach associated with the storage of payment card data.

## 1.3 Equipment Servicing, Trade-ins & Disposal

Notify the PCI Coordinator if an acquirer leased computer, communications equipment, or POS device involved in the payment stream needs to be sent to for trade-in, servicing, or disposal.

If the merchant is looking to dispose of a merchant-purchased POS device (not acquirer leased), it will need to be physically destroyed by a bonded disposal vendor that issues a "Certificate of Destruction" as per the Queen's Sustainability e-waste procedure.

Merchants are responsible for managing equipment for any specialized payment applications or service providers that they receive a Payment Card Acceptance Policy Exemption Approval for. This servicing and disposal should be coordinated directly with the provider and adhere to applicable Queen's policies.

In all other instances, the merchant may contact Queen's Sustainability to provide guidance for the destruction of electronic media.

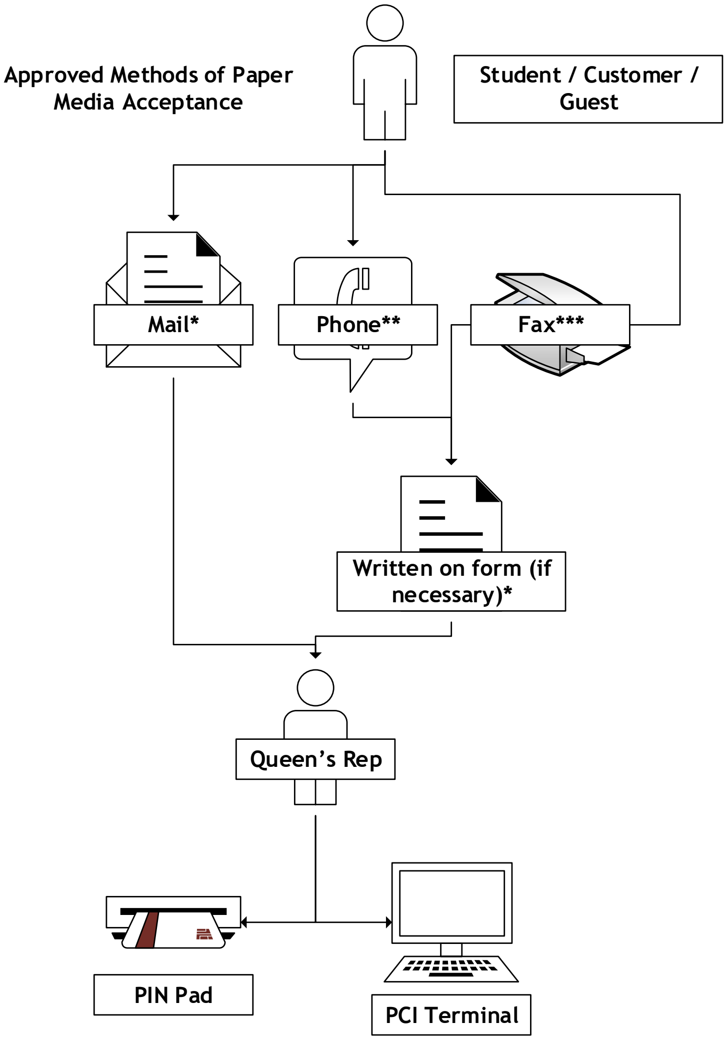
## 1.4 Electronic Media Records Retention

Merchants must ensure that a record is kept of every transaction, regardless of whether or not it is approved or declined. The record should include the date the payment card data was processed, how the transaction was processed (e-commerce, PCI terminal, POS device, etc.), who processed it (customer or an employee, contractor, or service provider operating on behalf of Queen's), the amount, and the brand of the card. This record must be retained for at least two years and in accordance with the Records Retention Schedules.

## 1.5 Approved Methods of Physical Media Acceptance

The only physical media the merchant is permitted to use is paper. This media may have the cardholder's name, the full PAN, and the expiration date if it is received in any of the following ways:

- MOTO:
    - Where the customer providers their payment card data via mail (not email) on an authorized Queen's form. The form should have the word CONFIDENTIAL at the top and contain a pattern or colouring to make it easily identifiable.
- Fax:
    - Where the customer provides their payment card data via facsimile on an authorized Queen's form. The form should have the word CONFIDENTIAL at the top and contain a pattern to make it easily identifiable. The fax machine must be connected through an analog phone line (never a computer network), located in a secure environment, and have access restricted. If the fax stores information in memory, it must be protected by a security code and a procedure must be in place to immediately delete the memory once the document is printed. Furthermore, the ability to send or receive payment card data by facsimile which is then converted to email is not allowed.


Approved Methods of Paper Media Acceptance
Student / Customer / Guest
Mail*
Phone**
Fax***
Written on form (if necessary)*
Queen’s Rep
PIN Pad
PCI Terminal

*The card verification value (also known as CVD, CVN, CVV, CVV2, CVC) is NEVER to be written down in any form. If this information is provided it must be destroyed immediately as per the destruction procedures below.

**If telephone processing involves technologies such as VOIP, wireless headsets, etc., it needs to be approved by the PCI Coordinator prior to use.

***Processing using a fax machine must be approved by the PCI Coordinator prior to use.

The merchant is responsible for the chain of custody for any payment card data that they accept by paper. Custody transfer via a bonded courier is permitted.

Payment card information is never to be received via end user messaging such as voicemail, e-mail, or text message.

## 1.6 Physical Media Storage

Paper physical media will be stored in a secured and locked cabinet in a restricted access area to prevent unauthorized access. It may not be retained either:

a) Once the transaction has been completed OR

b) Past 30 days

Merchants should conduct quarterly checks to ensure that no physical paper media has been retained past 30 days aside from the record of transaction.

### 1.7 Physical Media Destruction

Destroy paper physical media using a cross cut shredder. Disposal using an Iron Mountain shredding box is also acceptable.

### 1.8 Physical Media Records Retention

Merchants must ensure that a record is kept of every transaction, regardless of whether or not it is approved or declined. The record should include when the payment card data was received, who received it, who processed it, the date it was processed, the amount, the brand of the card, and the chain of custody (if transferred). This record must be retained for at least two years and in accordance with the Records Retention Schedules.

## 2.0 Merchant Accounts

### 2.1 Establishing Merchant Accounts with an Approved Acquirer

**Step 1:** Department, Faculty or Unit

Determine if a merchant account is necessary. If the department, faculty, or unit is looking to process payment cards for a one-time or annual event, they may refer to the One-Time Events Procedure for Accepting Credit Card Payments document and terminate this procedure here.

NOTE: Should the department, faculty, or unit choose to proceed in opening a merchant account, they must ensure they are aware of their responsibilities as outlined in the Payment Card Acceptance Policy.

**Step 2:** Department, Faculty or Unit

Complete the Requisition for a New Payment Card Facility. Ensure the form is approved and signed by the Business Officer. Email the completed requisition to the PCI Coordinator for approval.

NOTE: Departments, faculties or units are prohibited from entering into separate banking or payment processing services on their own, including PayPal, as per the Payment Card Acceptance Policy.

**Step 3:** PCI Coordinator

Conduct a review of the proposed payment stream with the department, faculty, or unit. Either deny, request revisions and/or additional documentation, or approve the requisition.

Advise the department, faculty, or unit of any equipment that needs to be procured to operate the new merchant account (ex. PCI terminal, POS devices). The merchant is responsible for the procurement of all equipment required to operate a merchant account **except** equipment that is leased by the acquirer, which will be coordinated by Financial Services.

Pre-fill the Declaration Document for the department, faculty, or unit.

**Step 4:** Department, Faculty or Unit

Once the requisition is approved, designate a PCI Merchant Contact for the new merchant account. This role will be responsible for coordinating the compliance activities (training, ethics agreements, user access, logs, etc.) on behalf of the department, faculty, or unit. Notify the PCI Coordinator.

**Step 5:** PCI Coordinator

Submit the request to open a new merchant account to the acquirer and facilitate the delivery of any acquirer provided equipment.

Initiate the support ticket request to connect the new account to the PCI network (if applicable). Copy the PCI Merchant Contact.

**Step 6:** ITS

Review the support ticket and advise the PCI Merchant Contact and PCI Coordinator of any additional equipment and/or wiring that needs to be ordered/installed (if applicable).

Complete wiring and network configuration changes and update support ticket with status of completed work.

**Step 7:** PCI Merchant Contact

Ensure any employees, contractors, and/or service providers operating on behalf of the University who will interact with the new payment stream receive the appropriate training and sign the Payment Card Security & Ethics Agreement. Request user access from the PCI Coordinator as required. Training requirements can be found on the Declaration Document.

Order and install equipment as advised by ITS and the PCI Coordinator. Ensure all pre-provided passwords are reset.

Complete the Declaration Document.

**Step 8:** PCI Coordinator & Financial Services

Alert the PCI Merchant Contact and Business Officer when the new account is active.

Verify that any employees, contractors, and/or service providers operating on behalf of the University have completed the appropriate training and signed the Payment Card Security & Ethics Agreement prior to fulfilling any requests for access to the new account. Close the support ticket.

## 2.2 Modify or Remove an Existing Merchant Account

**Step 1:** PCI Merchant Contact

Complete the Change/Close Form – Payment Card Facility. Ensure the form is approved and signed by the Business Officer. Email the completed form to the PCI Coordinator for approval.

**Step 2:** PCI Coordinator

Review form and either deny, request revisions and/or additional documentation, or approve.

**Step 3:** PCI Merchant Contact

Notify PCI Coordinator of any user accounts and/or PCI user IDs that need to be modified or removed.

**Step 4:** PCI Coordinator

Submit the request to modify or remove the merchant account and/or user access to the acquirer and facilitate the return of any acquirer provided equipment (if applicable).

Initiate the support ticket request to move/de-provision PCI jacks, PCI terminals, PCI User IDs, etc. (as applicable).

**Step 5:** ITS

Update the support ticket with status of completed work.

**Step 6:** PCI Coordinator

Alert the merchant and Business Officer when the account has been modified/closed. Close the support ticket.

**Step 7:** PCI Merchant Contact

Update the Declaration Document (if required).

## 3.0 Exemption Requests

### 3.1 Submitting a Payment Card Acceptance Policy Exemption Request to use a Non-Approved Payment Application or Service Provider

**Step 1:** Department, Faculty or Unit

Understand their responsibilities as a future merchant as outlined in the Payment Card Acceptance Policy.

NOTE: The University will provide a core level of service and support to merchants to facilitate the processing of payment card transactions using the PCI network as per the Payment Card Acceptance Policy. Should a merchant decide to use a specialized payment application for payment processing, the merchant will be responsible for any additional costs and resources arising from the use and implementation of the payment application. In addition, the merchant will also be responsible for any costs related to ensuring that the payment application and/or service provider is compliant with all payment card compliance standards.

**Step 2:** Department, Faculty or Unit

Email the PCI Coordinator and provide:

- The proposed service provider’s AOC (if the request is to use a non-approved service provider)
- The payment application’s certification of P2PE, PA DSS, or validation of compliance with the PCI Software Security Framework (if the request is to use a non-approved payment application);
- A copy of the draft contract (prior to signing) that outlines who is responsible for PCI requirements. The service provider must be willing to

indemnify the University for all costs related to a potential or actual security breach associated with the processing, storing, or transmission of payment card data;
- A description of the proposed payment stream;
- A summary of a costs associated with the proposed payment stream;
- An ATO from ITS;
- A completed Payment Card Acceptance Policy Exemption Request form.

**Step 3:** PCI Coordinator

Conduct a review of the proposed payment stream with the department, faculty or unit. Review documents provided and either deny, request revisions and/or additional documentation, or approve.

In cases where escalation is necessary, escalate to the CPPSC for guidance and/or authorization.

Advise the department, faculty, or unit of any equipment that needs to be procured to operate the new merchant account (ex. PCI terminal, POS devices). The merchant is responsible for the procurement of all equipment required to operate a merchant account.

Pre-fill the Declaration Document for the department, faculty or unit.

**Step 4:** Multiple

Proceed with steps 4-8 as outlined in section 2.1 Establishing a Merchant Account with an Approved Acquirer.

NOTE: Financial Services will not facilitate the delivery of any equipment for specialized payment applications or service providers.

## 3.2 Modifications and Terminations to Payment Applications and Service Provider Agreements

**Step 1:** PCI Merchant Contact

Email the PCI Coordinator and Business Officer about the modification or termination of the provider agreement.

**Step 2:** PCI Coordinator

Review the email and determine next steps. If necessary:

1. Request the department receive an updated SPRA to reflect the changes
2. Submit a support ticket to move/de-provision PCI jacks, PCI terminals, DSL modems, PCI User IDs, etc.

**Step 3:** PCI Merchant Contact

Update the Declaration Document (if applicable).

# 4.0 User Access

## 4.1 New User (Employee, Contractor, Service Providers acting on behalf of Queen's) Access

**Step 1:** PCI Merchant Contact

Payment card data should be shared with users on a *need-to-know* basis to perform their job duties. If it is determined that a user requires access to payment card data, a request should be emailed to the PCI Coordinator. Use the following qualifying questions to determine the level of access needed:

1. Will the user be interacting with payment card data over the phone?
    - If yes, do they then process the payment? See point 3.
    - If no, no access is required.
2. Will the user be handling payment card data in written form?
    - If yes, do they then process the payment? See point 3.
    - If no, no access is required.
3. Will the user be processing payment card data using a PCI terminal?
    - If yes:
        - Ensure appropriate training is completed and Card Payment Security & Ethics Agreement is signed.
        - Request a PCI User ID and access to the virtual terminal.
    - If no, see items 4-7.
4. Will the user be processing refunds on a PCI terminal?
    - If yes:
        - Ensure appropriate training is completed and Card Payment Security & Ethics Agreement is signed.
        - Request a PCI User ID and access to the virtual terminal.
    - If no, see items 5-7.
5. Will the user be ONLY processing refunds where the PAN is masked (with no access to payment card data)?
    - If yes:
        - Ensure appropriate training is completed and Card Payment Security & Ethics Agreement is signed.
        - Request access to the specific product where refunds will be performed.
    - If no, see item 6-7.
6. Will the user need access to reports pertaining to payment card data?
    - If yes:
        - Ensure appropriate training is completed and Card Payment Security & Ethics Agreement is signed.
        - Request reporting ONLY access. This will not require a PCI User ID.
    - If no, see item 7.
7. Will the user need to configure/maintain the cardholder data environment?
    - If yes:
        - Ensure appropriate training is completed and Card Payment Security & Ethics Agreement is signed.

    - ▪ Request access for the specific product that will be configured/maintained (ex. Hosted checkout, virtual terminal, etc.)
  - o If no, contact the PCI Coordinator for assistance.

NOTE: Users processing payments and refunds using a POS device must complete the PIN Pad Security Training. No user access is required.

NOTE: Merchants are responsible for managing user access for any specialized payment applications or service providers that they choose to engage outside of the University's approved Acquirer(s). User access to specialized payment applications must adhere to the PCI DSS requirements for user accounts.

These applications and providers must still be approved by the PCI Coordinator, and the PCI Coordinator will be responsible for requesting PCI user IDs if there is any payment processing over the PCI network.

**Step 2:** PCI Coordinator

Verify that the user has completed the necessary training and signed the Payment Card Security & Ethics Agreement. If yes:

- Submit the support ticket for the creation of a PCI user ID.
- Submit the request to the acquirer for the necessary access.

**Step 3:** ITS

Complete the support ticket and notify the user of their credentials.

**Step 4:** PCI Coordinator

Notify the PCI Merchant Contact when access has been created.

## 4.2 Modify/Terminate User (Employee, Contractor, Service Providers acting on behalf of Queen's) Access

User: Forgotten Password (PCI User ID)

Contact the IT Support Centre to have the password reset.

User: Forgotten Password (Acquirer)

Contact the acquirer's helpdesk. The PCI Coordinator can provide contact information.

PCI Merchant Contact: Terminate a User

Email the PCI Coordinator. They will submit the support ticket to deactivate the PCI user ID and/or revoke acquirer access. ITS will review the support ticket, remove the account and update the support ticket once the account is removed.

## 5.0 Incident Response

**Step 1:** Merchant, ITS

Observes a possible incident or breach. Some incident/breach indicators are:

- A secured, locked cabinet with payment card data has been broken into or looks damaged.
- Lost paper forms containing payment card data.
- Suspicious behaviour around devices
- A skimming device or unusual attachment on a POS device.
- A broken tamper proof seal on a POS device.
- Multiple small transactions (at the one dollar value) through an online store or e-commerce account.
- Multiple refunds going to the same card.
- Different serial numbers on the PIN pad machine indicating the device has been switched.
- Unfamiliar equipment surrounding your PCI terminal or POS device.
- A vulnerability appears in the weekly network scans.
- ITS find a possible issue during their daily checks of the PCI network and hosting environment.

**Step 2:** Merchant

Immediately stop taking payments on the compromised station and disconnect from the PCI network (if applicable). Only shut down the device if this is the only way to prevent the system from being connected to the network (like a cellular PIN pad).

Disconnect by unplugging the network cable, phone line, etc.

Do NOT resume processing payments until notified to do so.

**Step 3:** Merchant

Report the suspected breach or incident to:

a) During Business Hours: IT Support Centre at 613-533-6666.
b) After Business Hours: IT On-Call by emailing spnotice@queensu.ca. If you don’t receive a response within 30 min, contact 613-217-2474.

**Step 4:** ITS

Immediately alert the Information Security Officer, PCI Coordinator, and Business Officer using the methods indicated in the PCI Incident Response Plan.

**Step 5:** ISO & PCI Coordinator

Follow the PCI Incident Response Plan. This includes documenting the incident, validating the breach, controlling the breach, and notifying the card brands.

**Step 6:** PCI Coordinator

Once the threat has been resolved, notify the merchant(s) and Business Officer in writing that they may resume processing payments.

## 6.0 Compliance Activities

**Step 1:** Merchant

Designate a point of contact who will be responsible for PCI for each payment stream. This individual is the PCI Merchant Contact. They will be responsible for:

- Conducting weekly inspections of POS devices (includes card swipe devices, pay and display machines, PIN pads). This becomes a daily inspection if the devices are located in a publically accessible area or are left unattended.
  - These need to be logged and submitted to the PCI Coordinator every Mar, Jun, Sept, and Dec.
- Ensuring any paper physical media, POS devices, etc. are stored according to the proper procedures.
- Ensuring that those with access to payment card data have been appropriately trained and signed the Payment Card Security & Ethics Agreement.
- Ordering required PCI equipment.
- Requesting new user access.
- Requesting a termination of user access.
- Maintaining a PCI Staff Log of all employees, contractors, and/or service providers operating on behalf of Queen’s who have access to payment card data and their user access.
  - These need to be submitted to the PCI Coordinator every Mar, Jun, Sept, and Dec.
- Working with the PCI Coordinator to facilitate the annual PCI compliance audit documentation (Declaration Documents, SAQs, and AOCs).
  - Annually in Nov.
- Submitting any necessary service provider AOC, P2PE, or PA DSS documentation to the PCI Coordinator
- Reporting any violations of the Payment Card Acceptance Policy and/or Procedures to the PCI Coordinator.

**Step 2:** PCI Coordinator

Maintain a file with Merchant POS Inspection Logs, PCI Staff Logs, quarterly ASV scans, and annual compliance documentation (Declaration Documents, SAQs, and AOCs).

Remit quarterly ASV scans to the Acquirer.

Submit evidence of annual PCI compliance to the Acquirer.

**Step 3:** PCI Coordinator

Assess any reports of non-compliance, notify the Business Officer (and Information Security Officer as required) in writing, and determine remediation required.

## 7.0 Definitions

**Access Control**

The process of controlling access to applications at a granular level, such as per-user, per-group, and per-resources.[i]

**Acquirer**

Also referred to as “merchant bank,” “acquiring bank,” or “acquiring financial institution”. Entity, typically a financial institution that processes payment card transactions for merchants and is defined by a payment brand as an acquirer. Acquirers are subject to payment brand rules and procedures regarding merchant compliance.[i]

**Administrative Access**

Elevated or increased privileges granted to an account in order for that account to manage business rules, systems, networks and/or applications. Administrative access can be assigned to an individual or system account. Accounts with administrative access are often referred to as “superuser”, “root”, “administrator”, “admin”, “sysadmin” or “supervisor-state”, depending on the particular operating system and organizational structure.[i]

**Application**

The system, functional area, or problem to which information technology is applied. The application includes related manual procedures as well as automated procedures. Payroll, accounting, and management information systems are examples of applications.[i]

**Approved Scanning Vendor (ASV)**

Company approved by the Payment Card Industry Security Standards Council to conduct external vulnerability scanning services.[i]

**Attestation of Compliance (AOC)**

The AOC is a form for merchants and service providers to attest to the results of a Payment Card Industry Data Security Standard assessment, as documented in the Self-Assessment Questionnaire or Report on Compliance.[i]

**Authentication**

Process of verifying the identity of an individual, device, or process as a prerequisite to allowing access to resources in an information system. Authentication typically occurs using 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.[i]

**Authorization**

Access privileges granted to a user, program, or process or the act of granting those privileges (source: CNSSI-4009 )

In the context of a payment card transaction, authorization occurs when a merchant receives transaction approval after the acquirer validates the transaction with the issuer/processor.[i]

**Authorization to Operate (ATO)**

The ATO process provides a structure, templates and check-list to manage risk in adoption of cloud applications at Queen's University.

**Business Officer** The finance and/or operational authority for a department, faculty, or unit.

**Card Payment Processing Steering Committee (CPPSC)** An internal Queen's Committee that governs card payment policy and procedure within the University.

**Cardholder Data Environment (CDE)** The people, processes and technology that store, process, or transmit payment card data or sensitive authentication data.[i]

**Chain of Custody** The record of sequence of acceptance, control, storage, transfer, processing, and disposal of physical payment card data.

**Customer** Also referred to as a "student," "guest" or "cardholder." An individual or organization purchasing goods or services from a merchant.

**Data Breach** Also referred to as a "data compromise" or "compromise." Intrusion into a computer system where unauthorized disclosure/theft, modification, or destruction of cardholder data is suspected.[i]

**Declaration Document** An internal Queen's document that defines all elements of a payment stream. It can be obtained through the PCI Coordinator.

**Europay, MasterCard and Visa (EMV) Chip cards** EMV cards are smart cards (also called chip cards or IC cards) which store their data on integrated circuits rather than magnetic stripes, although many EMV cards also have strips for backward compatibility.

**Encryption** Process of converting information into an unintelligible form except to holders of a specific cryptographic key. Use of encryption protects information between the encryption process and the decryption process (the inverse of encryption) against unauthorized disclosure).[i]

**Firewall** Hardware and/or software technology that protects network resources from unauthorized access. A firewall permits or denies computer traffic between networks with different security levels based upon a set of rules and other criteria.

**Information Security Officer (ISO)** An internal Queen's staff member who operates the University's Cybersecurity Program and ensures compliance with the University's information security policies and regulatory environment.

**Information Technology Services (ITS)** An internal Queen's department that oversees the operation, servicing, and implementation of enterprise technology at the University.

**Issuer**

Entity that issues payment cards or performs, facilitates, or supports issuing services including but not limited to issuing banks and issuing processors. Also referred to as “issuing bank” or “issuing financial institution.”[i]

**Mail Order/Telephone Order (MOTO)**

Method for accepting payment cards that are either mailed or provider over the telephone.[i]

**Masking**

In the context of the Payment Card Industry Data Security Standard, it is a method of concealing a segment of data when displayed or printed. Masking is used when there is no business requirement to view the entire primary account number. Masking relates to protection of the primary account number when displayed or printed.[i]

**Merchant**

For the purposes of the Payment Card Industry Data Security Standard, a merchant is defined as any entity that accepts payment cards bearing logos of any of the five members of the Payment Card Industry Security Standard Council (American Express, Discover Financial Services, JCB International, MasterCard Worldwide, or VISA, Inc.) as payment for goods and/or services. Note that a merchant that accepts payment cards as payment for goods and/or services can also be a service provider, if the services sold result in storing, processing, or transmitting payment card data on behalf of other merchants or service providers.[i]

**National Institute of Standards and Technology (NIST)**

An American non-regulatory agency that provides a policy framework for security guidance.

**Payment Application**

A software application that stores, processes, or transmits cardholder data as part of authorization or settlement, where the payment application is sold, distributed, or licensed to third parties. Hardware is only included as part of the payment application if it is intertwined with the software (ex. part of a payment card swipe terminal).[i]

**Payment Application Data Security Standard (PA DSS)**

The PA DSS is for software vendors and others who develop payment applications that store, process or transmit payment card data and/or sensitive authentication data, for example as part of authorization or settlement when these applications are sold, distributed or licensed to third parties.[i]

**Payment Card**

*A*ny payment card/device that bears the logo of the founding members of Payment Card Industry Security Standards Council, which are American Express, Discover Financial Services, JCB International, MasterCard, or Visa, Inc.[i]

**Payment Card Brand** The respective financial entities (American Express, Discover Financial Services, JCB International, MasterCard Worldwide, or VISA, Inc.) responsible for advancing and promoting the Payment Card Industry Data Security Standard.

**Payment Card Data** At a minimum, payment card data (also known as cardholder data “CHD”) consists of a primary account number (PAN). Payment card data may also appear in the form of the PAN plus any of the following: cardholder name, expiration date, security code, and/or the card verification value (also known as CVD, CVN, CVV, CVV2, CVC).[i]

**Payment Gateway** A merchant service provided by an acquirer or payment processor that authorizes credit or debit card payment processing for e-commerce and online retailers.

**Payment Processor** Entity engaged by a merchant or other entity to handle payment card transactions on their behalf. While payment processors typically provide acquiring services, payment processors are not considered acquirers unless defined as such by a payment card brand.[i]

**Payment Stream** Encompasses the entire process for accepting payment cards in a merchant retail location (including stores/shops and e-commerce storefronts) and may include a payment terminal, an electronic cash register, other devices or systems connected to the payment terminal (for example, Wi-Fi for connectivity or a PC used for inventory), services with e-commerce components such as payment pages, and the connections out to a merchant bank.

**Payment Card Industry Data Security Standard (PCI DSS)** These standards cover technical and operational system components included in or connected to payment card data. If you accept or process payment cards, the PCI DSS apply to you.[i]

**Payment Card Industry PIN Transaction Security (PCI PTS)** PTS is a set of modular evaluation requirements managed by PCI Security Standards Council, for personal identification number (PIN) acceptance point of interaction (POI) terminals.[i]

**Payment Card Industry Security Standards Council (PCI SSC)** It is the governing organization and open forum responsible for the development, management, education, and awareness of PCI Security Standards.[i]

**PCI Software Security Framework** The framework is a collection of software security standards and associated validation and listing programs for the secure design, development and maintenance of modern payment software. It is composed of the PCI Secure Software Standard and the PCI Secure Software Lifecycle.[i]

**PCI Coordinator** An internal Queen’s staff member who coordinates the PCI compliance program and provides guidance to Queen’s merchants on issues pertaining to PCI compliance.

**PCI Merchant Contact** An individual operating on behalf of Queen’s to coordinate compliance for a specific merchant account. This role is responsible for maintaining compliance at the merchant level by managing user access, coordinating training, managing inventory, completing Point of Sale Inspection Logs, PCI Staff Logs, and reporting violations to the PCI Coordinator.

**PCI Network** A secured, segregated Queen’s network for the sole purpose of processing payment card data.

**PCI Staff Log** An internal Queen’s log that details the Queen’s employees, contractors, and/or service providers acting on behalf of the University who are involved in the acceptance, capturing, storage, transmittal, and/or processing of payment card data. The log includes a record of training, confirmation of a signed ethics agreement, and access levels/permissions.

**PCI Terminal** Hardware required to grant a Merchant’s e-commerce account access to the secure PCI Network. This is necessary in any instance where a merchant is entering payment card data into their e-commerce account on behalf of the cardholder.

**PCI User ID** Individual user access to login to the PCI network via a PCI terminal.

**Personal Identification Number (PIN)** Secret numerical password known only to the user and a system to authenticate the user to the system. The user is only granted access if the PIN the user provided matches the PIN in the system. Typical PINs are used for automated teller machines for cash withdrawal transactions. Another type of PIN is one used in EMV chip cards where the PIN replaces the cardholder’s signature.[i]

**Point of Interaction (POI)** The initial point where data is read from a card. An electronic transaction-acceptance product, a POI consists of hardware and software and is hosted in acceptance equipment to enable a cardholder to perform a payment card transaction. The POI may be attended or unattended. POI transactions are typically integrated circuit (chip) and/or magnetic-stripe card-based payment transactions.[i]

**Point of Sale (POS)** Hardware and/or software used to process payment card transactions at merchant locations. Examples include PIN pads, swipes, pay and display meters.[i]

**POS Inspection Log** An internal Queen’s log that details the inspections of hardware POS devices.

**Primary Account Number (PAN)** Unique payment card number (typically for credit or debit cards) that identifies the issuer and the particular cardholder account.[i]

**Qualified Security Assessor (QSA)** An external auditor qualified by PCI SSC to perform PCI DSS on-site assessments.[i]

**Self-Assessment Questionnaire (SAQ)** Reporting tool used to document self-assessment results of an entity’s business processes and compliance with the PCI DSS.[i]

**Security and Privacy Risk Assessment (SPRA)** An internal Queen’s tool used to determine and manage risk associated with the procurement of external goods and services. Part of the ATO process.

**Security Event** Any observable occurrence in a network or system. An example could be multiple failed log-ins.

**Security Incident** A violation or imminent threat of violation of computer security policies, acceptable use policies, or standard security practices. An example could be missing paper files with credit card data.

**Sensitive Authentication Data (SAD)** Security-related information used to authenticate cardholders and/or authorize payment card transactions, stored on the card’s magnetic stripe or chip.[i]

**Service Provider** Business entity that is not a payment brand, directly involved in the processing, storage, or transmission of payment card data. This also includes companies that provide services that control or could impact the security of payment card data. Examples include managed service providers that provide managed firewalls, intrusion detection systems (IDS), and other services as well as hosting providers and other entities. Entities such as telecommunication companies that only provide communication links without access to the application layer of the communication link are excluded.[i]

**Skimming Device** Also known as a “card skimmer.” A physical device, often attached to a legitimate card-reading device, designed to illegitimately capture and/or store the information from a payment card.[i]

**Support Ticket** A record of an issue that is logged in Queens' internal IT ticketing system. Support tickets are triaged and assigned to the appropriate party for resolution.

| | |
|---|---|
| Contact Officer | PCI Coordinator |
| Date Approved | September 14th, 2015 |
| Approval Authority | VPOC |
| Date of Commencement | September 14th, 2015 |
| Amendment Dates | Jan 2019 |
| Date for Next Review | Jan 2024 |
| Related Policies, Procedures and Guidelines | • Payment Card Acceptance Policy<br>• Electronic Information Security Policy Framework<br>• Electronic Information Security Policy<br>• Network and Systems Security Policy<br>• Records Retention Schedules<br>• Access to Information and Protection of Privacy Policy<br>• Payment Card Industry Data Security Standard |

[i] As defined by the Payment Card Industry Data Security Standard Glossary version 3.2 (2016)