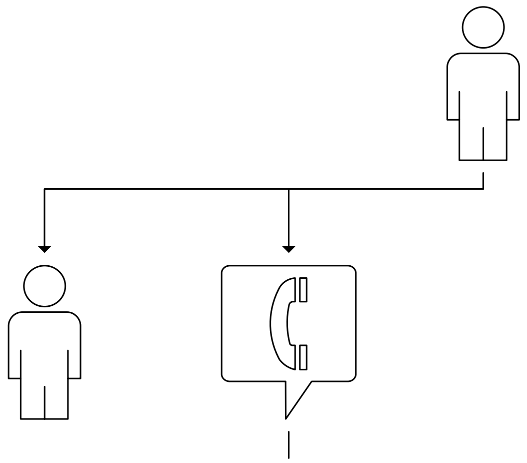
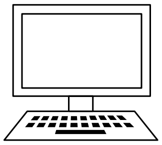
PAYMENT CARD ACCEPTANCE PROCEDURES

Contact Officer	PCI Coordinator





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 [illegible] (sp)-1.4)-2.6 (ic)

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.

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?
    -

        - Request access for the specific product that will be configured/maintained (ex. Hosted checkout, virtual terminal, etc.)
    - 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

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 613533-6666.
b) After BusinessHours: 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: Designate a point of contac t who will be responsible for PCI for each payment stream.
Merchant This individual is the PCI Merchant Contact. They will be responsible for:

x Conducting weekly inspections of POS devices (includes cns9ny scbrcCicncs heh03 0 T w C

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~~

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

Any 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).

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 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

Point of Sale (POS)	Hardware and/or software used to process payment card transactions

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