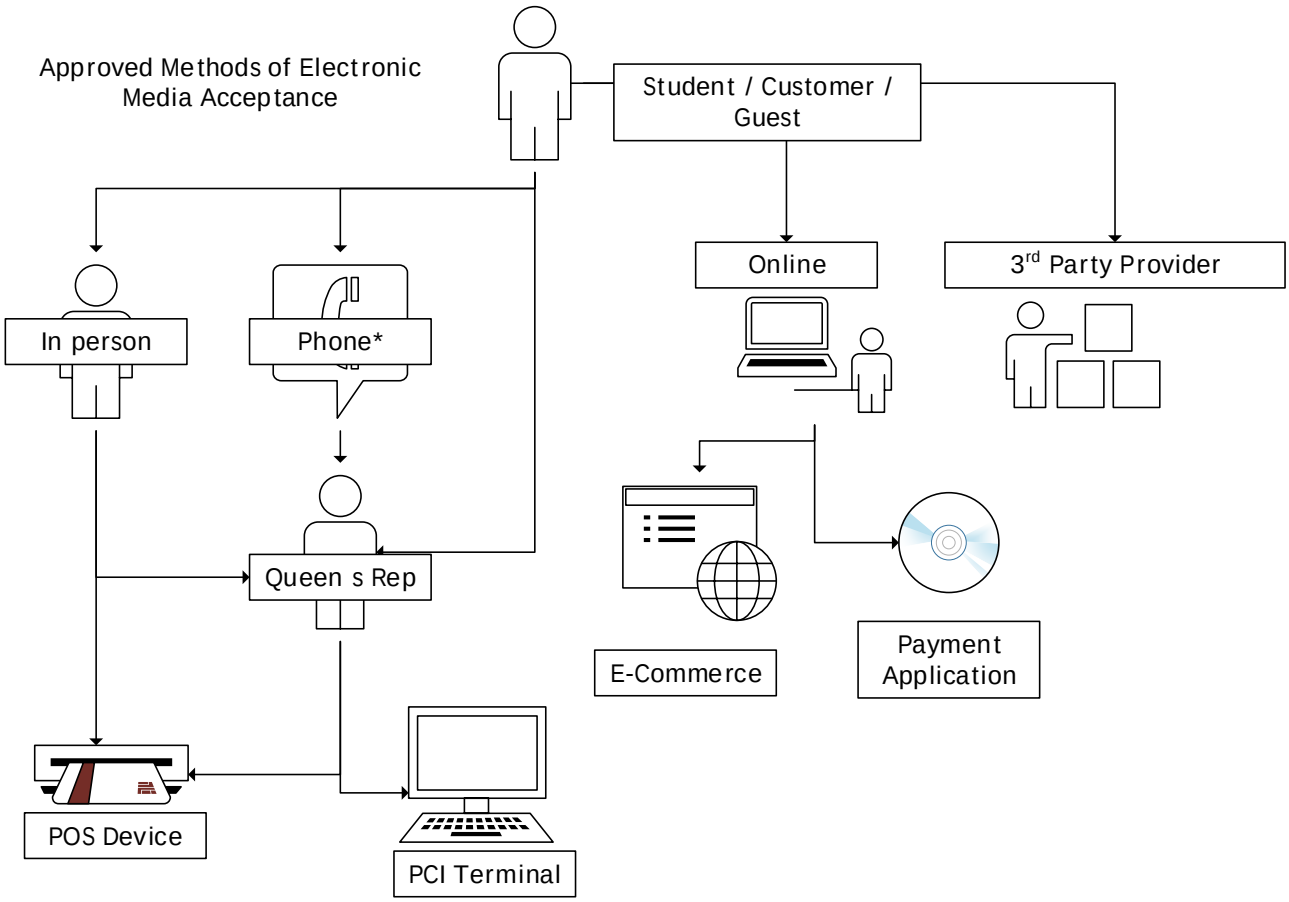
1.0 Approved Methods for Accepting 1.0



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

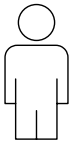
Merchants must ensure the security of electronic media. Remember to log off when away from them. If using a PCI terminal, log out as soon as transactions have been completed.

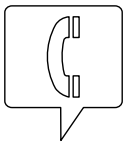
1.2 Approved Methods of Electronic Media Storage

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.





The card verification value (also known as CVD, CVN, CVV, CVV2, CVC) is NEVER 4(o)CVV,

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 Es

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 fou 462.67 Tm.04 Tf1 0 0 1 355.63 42 134.3 reW* nBT/F1 11.04 Tf1 0 0 1 19

Once

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-

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 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.

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.

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.

Issuer	Entity that issues pa

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.

	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

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	

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