Quick Guide for the Annual PCI Audit

As a primary contact, Business Officer, or IT resource associated with accepting card payments (in-person, by phone, online) you will be required to participate in the annual PCI audit.

The audit is a requirement of our preferred acquirer Chase and ensures we are compliant with Payment Card Industry (PCI) Data Security Standard (DSS).

> The following courses are offered on onQ for more detailed information:
>
> Introduction to Card Payment - Introduction to Card Payment (queensu.ca)
>
> Homepage - PCI-DSS Awareness Training (queensu.ca)
>
> Homepage - PIN Pad Security Training and Procedures (queensu.ca)

Each year you will receive by Merchant ID the applicable Declaration documents. The initial version will be in excel with multiple tabs to review and confirm. Items to be reviewed:

On the "Declaration 'type'" tab:

- Does the business description match align with the business process?
    - Does it describe all the methods used to accept cardholder data?
    - Is anything missing?
- Technical description is populated by the PCI Compliance Officer and ITS – will only need to be reviewed if your technical team has made changes to your payment stream without notifying the PCI Compliance Officer.
- Review the equipment used to input cardholder data (PIN pads, PCI terminals, etc.) – if applicable.
    - Have you recently changed devices?
    - Does all the information match the information on your device?
    - Is the location information accurate?
- Review the URLs used to collect payment card data via e-commerce/payment gateways – if applicable.
    - Are the Service Providers listed still in use?
    - Is the URL still accurate?
- Answer the questions.
    - AOC on File?
    - AOC Valid Through Date
    - PCI Exemption Request on File?

On the "Declaration – Workflow Diagram" tab:

- Does the workflow diagram include all the methods used to accept cardholder data as per the business description?
    - Are any steps missing?

On the "Declaration – Usage Policy" tab:

- Are the "Authorized parties approving use of technologies" still with Queen's University?
    - Are they still the correct individuals to contact to request changes on the merchant account?
    - Is there role still accurate?
- Ensure that the Personnel with access matches the current team members who interact with cardholder data.
    - Select their role from the drop-down that matches their responsibilities under the "**Roles & Training Required".** The training and documentation requirements for each specified role must be completed.
    - Select their Device from the drop-down menu.
    - Indicate their applicable Chase Processing Solutions, Reporting, and Refund Authorization access.
    - Training and/or ethics agreements are valid for 12 months. Ensure none extend beyond 12 months and have them updated where necessary.
    - The actual dates of training and attestation must be entered.
    - **If the staff member has not completed or updated the appropriate training, they are not permitted to interact with credit/debit card data until the training is complete.**