Payment Card Industry
Data Security Standards
(PCI DSS)

Awareness Training
What topics will this training cover?

- What is PCI DSS?
- Objectives of PCI DSS
- Common Terminology
- Background of PCI DSS
- 12 requirements of PCI DSS
- Policies and Procedures
- Key Responsibilities
- Merchant Requirements
- Information Received – Key Considerations
- PCI DSS Compliance
- PCI DSS Resources/Contacts
What is the Payment Card Industry (PCI) Data Security Standard (DSS)?

- The PCI Data Security Standard represents a common set of industry tools and measurements to help ensure the safe handling of sensitive information.
- It is comprised of 12 general requirements designed to:
  - build and maintain a secure network;
  - protect cardholder data;
  - ensure the maintenance of vulnerability management programs;
  - implement strong access control measures;
  - regularly monitor and test networks;
  - and ensure the maintenance of information security policies.
PCI DSS – Objectives

Why is PCI DSS Compliance important?

- Protection of cardholder data - Queen’s University has an obligation to students, vendors, alumni, and others to keep their cardholder information safe when processing credit card payments, and must comply with the PCI DSS standard

- Non-compliance with PCI DSS could result in:
  - Lost revenue & downtime for systems that are breached
  - Significant fines to Queen’s University by credit card companies allocated to responsible Queen’s departments
  - Liability for damages
  - Potential loss of credit card acceptance privileges
Training Objective - provide you with the knowledge and understanding needed to protect cardholder data.

Who should complete this training?

All University Staff who have any association with receiving payments through credit cards. This can include direct handling of credit cards, obtaining credit information over the phone, or payments accepted through third party e-commerce applications.

When should PCI DSS Compliance be considered?

Compliance should be factored into all dealings with a merchant account. It is an ongoing process, not a one-time event. Compliance helps prevent security breaches and theft of payment card data, not just today, but in the future as well.
PCI DSS – Common Terminology

- PIN Pads (formerly point-of-sale terminals)
- PCI Terminals (formerly Virtual Terminals)
- E-Commerce (formerly online Applications)
Established by the PCI Data Security Council - founded in 2006 by American Express, Discover, JCB International, MasterCard and Visa Inc.

Regulations apply to anyone who stores, processes, and/or transmits cardholder data.

Overall objective is to identify and correct vulnerabilities by ensuring appropriate levels of security are maintained.

Applies to all forms of payment card acceptance:
- Mail, phone, fax, PIN Pads, e-commerce, in-person.
Below are the 12 requirements that every entity processing credit card data must meet, as per PCI DSS:

<table>
<thead>
<tr>
<th>Goals</th>
<th>PCI DSS Requirements</th>
</tr>
</thead>
<tbody>
<tr>
<td>Build and Maintain a Secure Network</td>
<td>1. Install and maintain a firewall configuration to protect cardholder data</td>
</tr>
<tr>
<td></td>
<td>2. Do not use vendor-supplied defaults for system passwords and other security parameters</td>
</tr>
<tr>
<td>Protect Cardholder Data</td>
<td>3. Protect stored cardholder data</td>
</tr>
<tr>
<td></td>
<td>4. Encrypt transmission of cardholder data across open, public networks</td>
</tr>
<tr>
<td>Maintain a Vulnerability Management Program</td>
<td>5. Use and regularly update anti-virus software or programs</td>
</tr>
<tr>
<td></td>
<td>6. Develop and maintain secure systems and applications</td>
</tr>
<tr>
<td>Implement Strong Access Control Measures</td>
<td>7. Restrict access to cardholder data by business need to know</td>
</tr>
<tr>
<td></td>
<td>8. Assign a unique ID to each person with computer access</td>
</tr>
<tr>
<td></td>
<td>9. Restrict physical access to cardholder data</td>
</tr>
<tr>
<td>Regularly Monitor and Test Networks</td>
<td>10. Track and monitor all access to network resources and cardholder data</td>
</tr>
<tr>
<td></td>
<td>11. Regularly test security systems and processes</td>
</tr>
<tr>
<td>Maintain an Information Security Policy</td>
<td>12. Maintain a policy that addresses information security for all personnel</td>
</tr>
</tbody>
</table>
The policies and procedures that all merchant accounts must follow can be found at:

- Policy for the Acceptance of Credit and Debit Cards
- Procedures for the Acceptance of Credit and Debit Cards

These policies and procedures apply to all merchant accounts at Queen’s University. Some key points include:

- Departments may only accept payments through Merchant accounts established & approved by Financial Services
- Use of PayPal or other service providers is prohibited
Key Responsibilities

Financial Services
• Set up of all Merchant Accounts required by Queens departments
• Manage agreement(s) with payment card processing provider(s)
• Oversight & enforcement of policy & procedures through PCI Coordinator role
• Assistance with accounting for merchant account transactions
• Provide Training & Awareness regarding acceptance of card payments
• Coordination of receiving annual attestations and self-assessment questionnaires from Departments/Faculties
• Administer requested changes to existing Merchant Accounts

IT Services
• Provide core level of service and support to Merchants to facilitate processing of credit card transactions
Faculties/Departments with Merchant Account(s)

- Certificate of Credit Card Security and Ethics Agreement – to be signed by ALL users & submitted by department – now to be completed upon initial setup and for any new hires
- Annual Training – to be completed by all staff who have any association with receiving payments through credit cards. This can include direct handling of credit cards, obtaining credit information over the phone, or payments accepted through third party e-commerce applications.
- New Hires – the following must be completed before processing any cardholder data:
  - Background & Reference checks (CPIC’s recommended)
  - Training
  - Signed Certificate of Credit Card Security and Ethics Agreement
- Ensure all card transactions are handled in accordance with the Policy & Procedures regarding the Acceptance of Credit and Debit Cards
- Annual Attestation that merchant is compliant with the Queen’s policy & Procedures regarding card payment acceptance, and with PCI DSS
- Completion of PCI Self-Assessment Questionnaire (SAQ) – annually
- Comply with Merchant Requirements – listed in following slides
Key Responsibilities (con’t)

Staff Handling or Processing Cardholder Data

- Certificate of Credit Card Security and Ethics Agreement – to be signed by ALL users & submitted by department – now to be completed upon initial setup and for any new hires
- Annual Training – to be completed by all staff handling cardholder data
- New Hires – the following must be completed before processing any cardholder data:
  - Background & Reference checks (CPIC’s recommended)
  - Training
  - Signed Certificate of Credit Card Security and Ethics Agreement
- Ensure all card transactions are handled in accordance with the Policy & Procedures regarding the Acceptance of Credit and Debit Cards
- Comply with all Merchant User Requirements – listed in following slides
NEVER store full cardholder data in any form, for any reason, unless absolutely necessary.

Destroy the following information immediately after processing:

- Full Primary Account Number (PAN)
- Expiration date
- Track data (magnetic stripe data)
- CVV Code (3 digit security code)
- Personal Identification Number (PIN)

If you must store cardholder data, only store the last 4 digits of the PAN – in a secured location.
Storage of Cardholder Data (if absolutely necessary)

- Cardholder data (such as PAN or Expiry Date) can never be kept more than 30 days after the transaction

- Cardholder Authentication data (such as 3-digit ‘CVV Code’ on back of card) may only be retained until the transaction authorization is completed

- Any Cardholder data contained in any electronic storage must be rendered unreadable (through encryption, etc.)

- Any Electronic data storage must be inventoried annually

- Any Physical data storage must be reviewed quarterly
Only allow employees who have a legitimate business need to access cardholder information

Restrict physical access to areas where credit card information is handled and stored

For any cardholder data processed through a computer application, each user must have their own User ID, coupled with a secure password that is regularly changed.

Visual inspection of all PIN Pad machines for evidence of tampering must be done weekly
The following should be reported to the PCI Coordinator:

- Any planned changes to procedures and/or practices related to your acceptance and processing of card payments, including:
  - New merchant account required, or change in setup
  - Change in staff, storage, or any other procedural change
- Any suspicious behavior or indication of device tampering
- Any suspected breach or actual security incident
- Any identified incidence of non-compliance with policy and/or procedures related to acceptance of card payments
Email
- No request should ever be made for credit card information to be sent by Email. Any received by email should be deleted immediately, and cardholder should be informed we cannot process information received via email

Text Messaging
- Similar to email, no cardholder data should ever be sent/accepted by text

Phone
- Information received by phone should be entered directly into PCI terminal or PIN Pad and not written down whenever possible. If required to write the information down, it should be shredded immediately once processed
- If you provide a phone number for customers to call in with card information, the phone line used should not have voicemail capabilities
Fax
- Information should be received only by fax machines that are in locked areas only accessible by staff that process the information, and/or only received on fax machines that require passcodes to print any incoming faxes. If using fax as method of receiving info, contact the PCI Coordinator, who will review and approve on a case-by-case basis.

Mail/Paper Forms
- Do not store any card data that is not required
- Mark-out any card data so that it is illegible if on paper that needs to be kept/stored
- Where possible, detach part of form with card info and shred once transaction is processed
- Paper Forms should be received directly by staff processing them

E-Commerce
- Internal Applications used to collect data on sales should not collect, process, or keep any card data
Through the vigilance and efforts of all staff processing credit card information, Queen’s University will achieve and maintain full PCI DSS Compliance

- You are the 1st line of defense against fraud at Queen’s
  - Recognize unusual or suspicious activity/transactions
  - If you recognize procedures/regulations that are not being followed, contact the PCI Coordinator immediately
PCI Website – Queen’s

http://www.queensu.ca/financialservices/procedures/payment-card-industry-pci

PCI Security Standards Council

https://www.pcisecuritystandards.org/pci_security/

Contact:

Leisha Hawes (PCI Coordinator)
Manager, General Accounting (Financial Services)
E: pcicoordinator@queensu.ca
P: (613) 533-6000 x79563