B5009-1 CREDIT AND DEBIT CARD HANDLING PROCEDURES

1. **Credit Card Handling**
   - **1.1.** It is the responsibility of the manager/supervisor of each department to ensure that line staff meet the requirements of this policy.
   - **1.2.** It is the responsibility of the manager/supervisor of each department to ensure that the full primary account number (full PAN) or authentication data (magnetic stripe contents, card-verification code or PIN) of any credit card is not stored either in electronic or in hard copy form.
   - **1.3.** It is the responsibility of Financial Services to minimize the processing and transmission of credit card numbers wherever possible by using a third party to process online transactions.
   - **1.4.** If credit card information is received by email or fax, process the payment and instruct the customer to, in the future, pay by phone, web or in person. Delete the email or shred the fax copy, or if the document is required, redact the credit card information before storing the document.
   - **1.5.** Merchant copies of credit card slips must only contain masked (partial PAN) data. These records may be kept in a secure manner to facilitate resolving charge back items. Records are to be kept in accordance with Langara's Records and Information Management Policy. (Policy No. B5010)
   - **1.6.** Any credit card left by a customer should be properly secured by the department. The card should be held for a retention period (suggest five business days) to provide an opportunity for the customer to contact Langara and/or return and collect the card. Any cards unclaimed after the retention period should be shredded by the department.

2. **Credit Card Processing**
   - **2.1.** The PIN method (chip enabled cards) has strongest security and should be used for in person transactions. The magnetic swipe method should only be used for non-chip enabled cards.
   - **2.2.** Unless there is a prior approved process, do not enter credit card information directly into a software application such as Excel or a web browser.

3. **Payments by Phone**
   - **3.1.** It is recommended that departments only accept credit card payments by phone where there is recourse available in cases where the credit card payment is rejected (chargeback). If there is no recourse available, the department is accepting the chargeback risk.
   - **3.2.** Whenever possible, enter the credit card information directly into the credit card terminal without recording it separately. If separate recording of credit card information is required (for example when the terminal is in use), use a recording form only, in a location that restricts visual access from others, complete the transaction and shred the form.

4. **Equipment**
   - **4.1.** All processing equipment must be safeguarded against compromise including being tampered with or swapped. Ensure the credit card terminal is truncating the card account number so that only the last 4 digits are visible.
   - **4.2.** Access to processing equipment should be limited to authorized staff and secured when not in use.

5. **Admin Cards**
   - **5.1.** The point of sale Admin Card restricts access to various terminal functions including financial transactions like refunds and voids.
   - **5.2.** Store Admin Cards in a secure location.
   - **5.3.** Restrict access to the Admin Card to a minimum number of staff.

6. Refunds

6.1. Cash refunds for a credit card transaction are not permitted. (*this may not be current policy, and if not, this needs to be re-worded)*

7. Third Party Service Providers

7.1. Langara must ensure that any third party or service provider, be it a vendor, processor, software provider, payment gateway or other service provider adhere to the same security requirements as Langara.

7.2. If cardholder data is shared with service providers, and/or if a service provider does business on behalf of Langara, the following policies and procedures must be followed:

7.2.1. A current and accurate list of service providers will be maintained, complete with contact information of relevant personnel. This list will be maintained by Financial Services.

7.2.2. For any service providers that may affect or have a relationship or function associated with Langara's cardholder data environment, the written agreement shall include an acknowledgement by the service provider of their responsibility for securing cardholder data, and statement of their PCI compliancy.

7.2.3. If the service provider will be processing, transmitting or storing cardholder data, they must provide evidence of their compliance to PCI-DSS.

7.2.4. Proper due diligence must be exercised before engaging with any service providers that may affect or have a relationship or function associated with Langara's data environment.

Related policies:

B5009 - Credit and Debit Cardholder Security Policy http://www.langara.bc.ca/about-langara/policies/policies/administration.html