B5009 – CREDIT AND DEBIT CARDHOLDER SECURITY

FINANCE/CREDIT AND DEBIT CARD HANDLING PROCEDURES

Credit Card Handling

1) It is the responsibility of the manager/supervisor of each department to ensure that all employees involved in handling card holder information are aware of and meet the requirements of these procedures. These procedures must be reviewed with all new staff and reviewed annually with all staff.

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.

3) It is the responsibility of Financial Services to minimize the processing and transmission of credit card numbers by the College wherever possible by using a third party to process online transactions.

4) Credit card information must not be received or submitted by email or FAX. Any email or fax submissions that contain credit card information will be deleted permanently and/or shredded, unless the document is required for some other legitimate business reason. In this case, redact the credit card information before storing the document. Redaction must be done prior to photocopying or scanning a document. The submitting client will be informed their transaction was not successfully processed. They will be advised of other compliant options.

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)

6) Any credit card left by a customer should be properly secured by the department. The card should be held for a retention period (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.

Credit Card Processing

7) The PIN and TAP methods (chip enabled cards) have the strongest security and should be used for in-person transactions. The magnetic swipe method should only be used for non-chip enabled cards.

8) Unless following a previously approved PCI compliant process, credit card information shall not be directly entered into a software application such as Excel or a web browser.

Payments by Phone

9) Credit card payments can only be accepted by phone using Langara's Interactive Voice Response (IVR) service (third party). This ensures that the payment processing is not transmitted over the Langara phone network.

Equipment

10) All processing equipment must be safeguarded against compromise including being tampered with or replaced. Ensure the credit card terminal only displays the last 4 digits of the credit card account number.

11) Employees will examine devices every day for attempted tampering and will report any issues or devices requiring replacement.

12) Only authorized staff shall have access to processing equipment. Processing equipment will be secured when not in use.

13) Financial Services will maintain a list of processing equipment that is reviewed annually.

Admin Cards

14) Admin Cards shall be stored in a secure location in a manner that restricts access to various terminal functions, including financial transactions like refunds and voids.

15) Access to the Admin Card will be restricted to those staff authorized to perform administrative functions.

Refunds

16) Cash and cheque refunds for a credit card transaction are not permitted.

Third Party Service Providers

17) 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:

    a. 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.

    b. 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 compliance.

    c. All service providers that process, transmit or store cardholder data must provide evidence of their compliance to PCI DSS.

    d. Proper analysis, investigation and proof of PCI DSS compliance must be completed before engaging with any service providers that may affect or have a relationship or function associated with Langara's data environment.