Title	**Credit and Debit Cardholder Security**
Number	**B5009**
Category	**Administration**

1. PURPOSE

To protect the credit and debit cardholder information of any individual or entity that utilizes a credit or debit card to transact business with the College. To ensure all credit card processing activities and related technology comply with Payment Card Industry Data Security Standards (PCI DSS)

All card processing activities and related technologies must comply with the Payment card Industry Data Security Standards (PCI DSS).

2. DEFINITIONS

Cardholder information – the contents of the magnetic strip, the primary account number plus any of the following: cardholder name, card expiration date, service code.

End user Messaging Technologies – Email, instant messaging, text messaging, chat.

Primary Account Number (PAN) – the unique number on a credit card that identifies the issuer and the cardholder account; also referred to as an "Account Number".

Payment Card Industry Data Security Standards (PCI DSS) – is a global initiative for the purpose of securing credit and banking transactions through an evolving set of mandatory requirements and guidelines covering security, policies, procedures, network/software design and other critical protective measures. These standards were developed in 2004 by a consortium of credit card providers (Visa, MasterCard, etc.), in an effort to reduce credit card fraud. PCI DSS Requirements

Personal Identification Number (PIN) – is a numeric password used to authenticate an individual to a system.

3. POLICY

Scope

3.1 This policy is applicable to all Langara staff members with access to cardholder information and departments who accept payment cards for payment by means including Internet (gateway provider), face to face (point of sale terminals), and non-face to face (information provided via other electronic means; fax, email, etc.).

General

3.2 The College is committed to protecting and preserving the privacy and security of cardholder information collected and processed in the conduct of business operations.

3.3 The College requires all staff and departments that process, store or transmit credit or debit card data to maintain compliance with PCI DSS.

3.4 Only authorized staff may accept and/or access credit or debit card information.

3.5 Individuals who have access to credit or debit card information are responsible for protecting the information.

3.6 Individuals are not permitted to retain credit card numbers or authentication data (magnetic stripe contents, card-verification code or PIN) in physical or digital form (hard copy or electronic). Retention includes paper or electronic files on any device (server, PC, laptop, smart phone, etc.).

3.7 Unprotected PANs are not to be transmitted without exception.

3.8 Third parties that Langara engages to do business on its behalf, which includes processing credit card transactions, must be compliant with this policy.

3.9 Approval from the Director, Financial Services is required before a credit card merchant account can be established and/or prior to the implementation of an e-commerce solution (e.g., software, systems, or applications with a payment feature).

3.10 An e-commerce solution must be approved by the Chief Information Officer or his/her delegate to ensure compliance with the College's technical standards and PCI DSS requirements.

3.11 All equipment and hardware used for the processing and transmitting of credit card transactions must meet applicable PCI DSS requirements.

3.12 All devices used to capture payment cardholder information must be protected against tampering. Front line employees must monitor these devices daily for attempted tampering or replacement of devices and report any anomalies or suspected tampering to their Supervisor for immediate communication to Financial Services.

3.13 All staff that handle cardholder information must be familiar with the Cardholder Data Security Incident Response Procedures.

3.14 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 and PCI compliance requirements as Langara.

4. RESPONSIBILITY

For inquiries relating to this policy, contact the Director, Financial Services.

5. REGULATIONS/PROCEDURES

PCI DSS Requirements

Cardholder Data Security Incident Response Procedures

Finance/Credit and Debit Card Handling Procedures

History/Revision	
Origination Date	November 4, 2017
Amendment Date(s)	June 11, 2019
Next Review Date	June 11, 2021