CAPILANO UNIVERSITY	POLICY		
Policy No.	Officer Responsible		
B.211	**Vice-President, Finance and Administration**		
Policy Name			
Credit and Debit Card Policy			
Approved by	Replaces	Category	Next Review
Board	**New**		**February, 2028**
Date Issued	Date Revised	Related Policies and Procedures	
September 24, 2019	**February, 2023**	**B.211.1 Credit and Debit Card Procedures** **B.210 Cash Policy**	

1. PURPOSE

The purpose of this policy is to

a) protect credit and debit cardholder information for individuals and entities that use credit and debit cards to transact business with Capilano University ("University"), and

b) ensure all credit and debit card processing activities and related technology follow *Payment Card Industry Data Security Standards* (PCI DSS) best practices.

2. DEFINITIONS

"Cardholder information" the contents of the magnetic strip, the primary account number plus any of the following, cardholder name, card expiration date and service code, for a credit, debit or other bank card.

"Primarily account number (PAN)" the unique number on a credit or debit card that identifies the issue or and the cardholder account, also refer to as an account number.

"Payment Card Industry Data Security Standards (PCI DSS)" global standards for securing credit and banking transactions with mandatory requirements and guidelines covering security, policies, procedures, network/software design and other critical protective measures.

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

3. SCOPE

This policy applies to employees who have access to cardholder information and departments that accept credit and debit card payments using a gateway provider, point of sale terminal, or other electronic means.

4. POLICY

4.1 The University is committed to protecting and securing cardholder information.

4.2 The Vice-President, Finance and Administration is responsible for implementing, administering and ensuring compliance with this policy and any related procedures.

4.3 The Vice-President, Finance and Administration has appointed the Director, Financial Services to design and implement:

a) procedures for processing and handling cardholder information to make sure that all employees and locations that process, maintain or transmit cardholder information do so in a manner that follows PCI DSS best practices, and
b) incident response procedures that employees must follow in the event of a security incident or suspicious transaction or event involving cardholder information.

4.4 Only those employees and locations authorized by the Vice-President, Finance and Administration and identified in *B.211.1 Credit and Debit Card Procedures*, may accept and/or access cardholder information. Employees and departments so authorized are responsible for protecting such cardholder information.

4.5 Employees are not permitted to

a) retain credit and debit card numbers or cardholder information in a physical or digital form (e.g. hard copy, paper, electronic file on any device such as server, PC, laptop or smartphone),
b) accept cardholder information by mail, e-mail, text or fax, or
c) transmit or communicate an unprotected or non-encrypted PAN or PIN.

4.6 The Director, Financial Services must approve all credit card merchant accounts and any significant changes to existing e-commerce solutions prior to implementation of e-commerce solutions for credit and debit card transaction processing.

4.7 The Chief Information Officer or designate must approve all e-commerce solutions and any significant changes to existing e-commerce solutions to make sure that related software and equipment comply with the University's technical standards and follow PCI DSS best practices. Third-party e-commerce solutions must be PCI-DSS compliant.

4.8 All equipment used to process cardholder information must be protected against tampering. Managers and supervisors of services at the University that are authorized to process card holder information must put processes in place to monitor equipment daily and report any anomalies or suspicions of tampering immediately to the Director, Financial Services.

4.9 Contracts with third parties engaged by the University to do business on its behalf, who process credit and debit card transactions must include the requirement to demonstrate PCI compliance by providing evidence of compliance annually.

4.10 The Director, Financial Services must make sure that third parties, service providers, vendors, payment gateway and other providers comply with PCI DSS requirements.

4.11 Cash transactions must be processed in accordance with the *B.210 Cash Policy*.

4.12 Exceptions to this policy must be jointly authorized in advance by the Vice-President, Finance and Administration and the Director, Financial Services and reported to the Finance Committee.

5. DESIGNATED OFFICER

The Vice-President, Finance and Administration is the Policy Owner responsible for the oversight of this Policy. The administration of this Policy and the development, subsequent revisions to and operationalization of any associated procedures is the responsibility of the Director, Financial Services.

6. REVIEW AND AMENDMENT

This Policy and associated procedure will be reviewed on a regular basis and amended as required in accordance with Policy B.102 Policy Development and Management.

7. REFERENCES

B.211.1 Credit and Debit Card Procedures
B.210 Cash Policy
Payment Card Industry Data Security standards (PCI DSS)