CAPILANO UNIVERSITY	PROCEDURE	
Procedure No.	Officer Responsible	
B.211.1	**Vice-President, Finance and Administration**	
Procedure Name		
Credit and Debit Card Procedures		
Policy This Procedure is Under		Date of Next Policy Review
B.211 Credit and Debit Card Policy		**October 2022**
Date Issued	Date Revised	Related Policies, Reference
October 2, 2019		**B. 210 Cash Policy** **Payment Card Industry Data Security standards (PCI DSS)**

1. PURPOSE

These procedures describe how credit and debit card transactions must be processed and cardholder information protected and secured, in accordance with *B.211 Credit and Debit Card Policy.*

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

These procedures apply to employees who have access to cardholder information and locations that accept credit and debit card payments using a gateway provider, point of sale terminal, or other electronic means**.**

4. PROCEDURES

Authorized locations and employees

4.1 In accordance with section 4.3 of the *B.211 Credit and Debit Card Policy,* "authorized locations" that can process credit and debit card transactions and handle cardholder information are restricted to

a) Financial Services,
b) Bookstore,
c) Centre for Sports and Wellness,
d) Continuing Studies,
e) Library,
f) Sunshine Coast campus, and
g) Theatre/Box Office

4.2 The manager/supervisor of each authorized location will ensure that employees who process credit and debit transactions and handle cardholder information and equipment

a) sign Appendix 1 – Acknowledgement of Understanding confirming that they have read and understand these procedures, *B.211 Credit and Debit Card Policy*, and the process to be followed in the event of a real or perceived security incident involving cardholder information and/or processing equipment.
b) have been trained to use credit and debit transaction processing equipment and to safeguard cardholder information, and
c) know when and how to use *Appendix 3 Cardholder Security Incident Response Process* in the event of a security breach involving cardholder information or credit and debit card processing equipment.

4.3 The manager/supervisor of each authorized location will complete *Appendix 2 Cardholder Security Contact and Response Information* each year and review the information with each employee authorized to process credit and debit card transactions and handle cardholder information and equipment.

4.4 Employees involved in processing credit and debit transactions and handling cardholder information and equipment will ensure that

a) the full primary account number (full PAN) and authentication data (magnetic strip contents, card verification code or PIN) for any credit or debit card is never stored in a physical or digital form (e.g. hard copy, paper or electronic file on any device such as server, PC, laptop or smartphone),
b) cardholder information is never received or transmitted by mail, email, text or fax. If such information is inadvertently transmitted by email or fax
    i) it must be promptly deleted or destroyed, unless required for some valid business purpose wherein all cardholder information must be redacted prior to storage or reproduction, and
    ii) the customer must be notified that the payment information has not been accepted and advised of other acceptable payment options,
c) merchant copies of credit card slips only contain masked (partial PAN) information. These records may be kept in a secure manner in order to facilitate resolving charge back items, and
d) credit or debit cards left by customers are properly secured for a retention period not to exceed five days, during which time efforts must be made to return the card to the

customer. Any unclaimed credit or debit cards must be destroyed immediately after the retention period unless alternate recovery arrangements have been made with the customer.

4.5 The Director, Financial Services will conduct an annual review to ensure compliance with these procedures.

Credit and debit transaction processing and refunds

4.6 PIN and TAP methods (i.e. chip-enabled cards), having the strongest security, should be used for in-person transactions. The magnetic slide method should only be used for non-chip enabled cards.

4.7 Credit and debit card transactions must never be refunded by cash or cheque.

Credit and debit card processing equipment

4.8 All credit and debit card processing equipment must be safeguarded from theft, tampering or damage at all times.

4.9 Credit and debit card processing equipment must

a) be restricted to employees with appropriate knowledge and training as identified in section 4.2,
b) be secured from the public when not in use,
c) never be left unsecured and unattended in a location with public access, and
d) be examined each day for evidence of tampering or damage.

4.10 The Director, Financial Services will ensure that detailed equipment lists are maintained for all credit and debit card transaction processing equipment.

4.11 The manager/supervisor will

a) update the equipment list for the authorized location immediately when equipment changes occur, and
b) confirm the equipment list by visual inspection or physical count each day.

4.12 Any evidence of tampering or damage to credit and debit card processing equipment must be reported immediately in accordance with *Appendix 3 Cardholder Security Incident Response Process.*

Third party service providers

4.13 If cardholder information is shared with third-party service providers and/or if a third-party service provider does business on behalf of the University, the Director, Financial Services, in collaboration with the Chief Information Officer, IT Services, will

a) perform proper analysis, investigation and proof of PCI DSS compliance before engaging any such third-party service provider,
b) obtain a written agreement from each third-party service provider acknowledging their responsibility for securing cardholder information and complying with PCI DSS,
c) ensure that IT Services contact information is provided to the service provider for the purposes of receiving relevant cybersecurity information,
d) maintain an accurate list of such third-party service providers, complete with contact information for relevant personnel, and
e) ensure that all third-party service providers provide evidence of compliance with PCI DSS each year.

4.14 Exceptions to this procedure must be jointly authorized in advance by the Vice-President, Finance and Administration and the President and reported to the Finance and Audit Committee.

5. RELATED REFERENCES

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

Appendix 1 – Acknowledgement of Understanding

I hereby acknowledge that I have read and understand the following policies and procedures relating to the processing and storage of credit and debit cardholder information

- *B.211 Credit and Debit Card Policy*
- *B.211.1 Credit and Debit Card Procedures*
- *Appendix 2 – Cardholder Security Contact and Response Information*
- *Appendix 3 - Cardholder Security Incident Response Process*

I acknowledge and understand that

- credit and debit cardholder information must always be processed and stored in a secure environment as specified in the University's policies and procedures
- credit and debit card transactions may only be processed or accepted in authorized locations and must be performed by authorized employees
- in the event of a real or perceived security breach or other suspicious transaction involving credit and debit card holder information, I must immediately report the event as prescribed in *Appendix 3 - Cardholder Security Incident Response Process*

Employee Name	Title/position
Employee Signature	**Date**

Appendix 2 – Cardholder Security Contact and Response Information

Authorized location (department)		
	Name	**Telephone number**
Primary contact at location		
Alternate contact at location		
Primary contact at Financial Services		
Primary contact at IT		
Primary contact at Campus Security *(Campus Security must be contacted if the incident involves an imminent danger or physical threat)*	*Emergency & non-emergency*	
Local police contact *(Police must be contacted if the incident involves an imminent danger or physical threat)*	*Emergency & non-emergency*	

Business recovery and continuity procedures for physical input devices	
POS/PIN pad and electronic application systems	• Discontinue using the POS device • Where possible, immediately discontinue using the affected application system • Contact IT • Disconnect affected device from network or telephone line as instructed by IT

All real or suspected security incidents involving cardholder information and credit/debit card transaction processing equipment must be reported immediately using the *Cardholder Data Security Incident Response Process* (see Appendix 3).

All contacts with cardholders and service providers concerning security incidents must be coordinated through Financial Services.

Manager/Supervisor name	**Title/position**
Manager/Supervisor signature	**Effective Date**

Appendix 3 - Cardholder Security Incident Response Process

The process described below must be used to address any security incidents that involve the unauthorized disclosure or modification of cardholder information.

Any malicious attempt to compromise the confidentiality or integrity of cardholder data, whether successful or not, is within scope for this process.

All real or suspected security breaches or incidents involving credit and debit cardholder information or transactions must be reported immediately as described below.

Process

If you discover or suspect a security breach or incident involving credit and debit cardholder information or equipment used to process such equipment, **immediately**

1. Contain or limit further exposure to the incident where possible. Stop using the equipment for transactions and/or taking payments and advise other staff accordingly
2. Contact IT Services at extension 4952 or externally at 604-984-4952 as soon as possible
3. Disconnect compromised systems from the network if instructed by IT Services. Otherwise, do not alter or access any systems until advised to do so
4. Secure the equipment and any paper records from continued use and for subsequent examination
5. Contact Financial Services at extension 1786 or externally at 604-984-1786 as soon as possible
6. Complete the *Cardholder Information Incident Report* and submit it to Financial Services and IT Services as soon as possible

If the incident is deemed to be solely related to e-commerce solutions, the incident response will be led by the Chief Information Officer, IT Services, or their designate, and will follow the IT Services cybersecurity incident response protocol. For incidents not involving technology solutions, the Director, Financial Services will:

1. Validate and assess the incident
    - Establish how it occurred, the source and time frame
    - Document the type of cardholder information that was breached (e.g. PAN, PIN, magnetic strip, expiration date, etc.)
    - Determine or approximate the number of cardholders affected
2. Advise senior management on an ongoing basis
3. Immediately report the incident to
    - the Privacy Officer and Legal Services
    - legal authorities as warranted
    - all affected service providers
4. In consultation with Communications, prepare and implement a plan for communicating the incident to affected cardholders (note: any such plan must be approved by the Vice-President, Finance and Administration)
5. When appropriate, confirm that the incident has been contained

Cardholder Information Incident Report

Incident location (Dept)		
Incident date and time (first observed or suspected)		
	Name	Telephone number
Primary contact at incident location		
Alternate contact at instant location		
Primary contact at Financial Services		
Primary contact at IT		
Describe how the incident was discovered and by whom?		
Describe any contact regarding the incident with Campus Security and local police*)*		
Select and describe the type of incident that occurred		
Was cardholder data involved? If so, describe what type	Last 4 digits of credit card	
	Cardholder name	
	Card type (Visa or Mastercard)	
Was sensitive authentication data involved?	Full magnetic stripe data	Answer Yes or No only
	CVV	Answer Yes or No only
	PIN	Answer Yes or No only
	Unsure/Unknown (describe)	
If possible, estimate the number of people or records impacted		
Does the incident compromise business operations continuity? If so, describe how.		
Is there a need for client or customer notification?		

Employee name (preparing this report)	**Title/position**
Signature	**Report Date**