Table of Contents

Use this privacy impact assessment (PIA) template prior to starting a new University Initiative or significantly changing an existing initiative involving the processing of Personal Information by VIU or a Third Party contracted by VIU. A University Initiative includes any activity or commitment undertaken by a University Employee in the performance of their duties that involves collection or processing of Personal Information. It may be, among other things, a program, service, or activity of the University, including the use or purchase of a technological solution or software for University activities (irrespective of the dollar value of the initiative).

Please read through this form before starting to populate it in order to ensure information is recorded in the correct sections.

PART 1: GENERAL INFORMATION

Initiative title:	VIU Campus Store POS System Upgrade ~~PrismRBS~~
Department or Faculty ("Business Unit"):	Bookstore, Ancillary Services
Initiative Lead (PIA drafter):	

Initiative Lead email:	
One-over-One Name and Title:	
One-over-One email:	
Privacy Officer name:	
Privacy Officer email:	
If initiative involves a Third Party (i.e. vendor, consultant, partner), provide:	Yes
1. Third Party name	~~PrismRBS~~ **Chase** Merchant Services
2. Product name (if applicable)	~~PrismCore, PrismPOS, WebPOS~~ Chase Paymentech Solutions Inc.
3. Third Party contact name and email	Glenn Graham, ~~Charles Hullett~~, Glenn.Graham@chasepaymentech.ca ~~chullett@prismrbs.com~~
4. Third Party URL	~~https://www.prismrbs.com/~~ www.chasepaymentech.ca

1. What is the initiative? Summarize what you are doing, how it works, who is involved and when or how long your initiative runs.

The purpose of the project is to update the Point of Sales (POS) component of the operating system used in the Campus Store. The legacy POS called WinPOS is outdated and at end of life. The new and updated version is called PrismPOS. WinPOS and the updated version called PrismPOS are components of the Prism Suite system, used to capture sales and inventory information.

2. Is this an administrative/operational, or teaching and learning initiative? Select all that apply.

- ☒ Administrative/Operational
- ☐ Teaching and Learning
- ☐ Research (Contact Privacy Office before continuing past Question 9)

3. If the initiative involves processing of Personal Information by a Third Party, does the initiative involve integration with VIU IT systems or other Third Party systems (i.e. a separate payment processor)?

- ☒ Yes
- ☐ No
- ☐ N/A

If yes, list them here:

Not VIU IT Systems

Vendor solutions:

- ~~FreedomPay-payment processor~~
- ~~PrismRBS~~
- Chase payment solution

4. What is the scope of the PIA?

Campus Store Point of Sale System Upgrade – Chase payment solution

5. Has a PIA previously been completed for this initiative?

☒ Yes
~~☐~~ A PIA was completed for the PrismRBS component and the FreedomPay component
This PIA is for the Chase payment processing component
☐ No
~~☒~~
☐ Not sure

6. What activities occur within the initiative?

Upgrading the existing POS System – due to end of life for this version of the System
Support from the vendor is no longer available

7. What are the data or information elements involved in your initiative? Please list all the elements of information or data that you might collect, use, store, or disclose as part of your initiative. Please indicate whether the Personal Information is required for the initiative or optional. Indicate whether the Personal Information is required by VIU, by the Third Party (i.e. for individual to have a vendor account/profile), or both.

~~All of the information listed is "Required".~~

~~Accounts could include:~~

- ~~Sponsor Information – student sponsors~~
- ~~Sponsored Students~~
- ~~Web Clients – ordering over the web – address, name, phone number~~

~~Payment information is encrypted~~

~~Shift 4 – product used to process payments; part of the PrismWeb Cloud environment~~

8. Did you list Personal Information in question 7? Personal Information is any recorded information about an identifiable individual, other than business contact information. Personal Information includes information that can be used to identify an individual through association or reference.

☐ Yes
☒
☐ No

9. If you answered "No" to question 8, how will you ensure that you do not unintentionally collect Personal Information?

If there is Personal Information involved in this initiative, continue to complete the remaining sections of the PIA. If there is not any Personal Information involved in this initiative, please submit questions 1-9 to the Privacy Officer along with the completed Signatures page.

PART 2: COLLECTION

FIPPA sets out requirements and restrictions related to collection of Personal Information by public bodies and their employees. Unauthorized collection is prohibited. This section will help you identify the legal authority for collecting Personal Information, and confirm that all Personal Information elements collected are necessary for the purpose of the initiative.

10. Whose Personal Information is collected in this initiative? Check all that apply.

- ☐ Students
- ☐ Prospective students
- ☐ Former students
- ☐ Alumni
- ☐ Employees (including casual services contractors or volunteers)
- ☐ Former employees (including casual services contractors or volunteers)
- ☐ Donors
- ☐ Other (specify): Student Sponsor
- ☐ Other (specify):

11. Is the information collected for a limited period of time or ongoing?

- ☐ Limited period: One or more times in a semester / quarter
- ☐ Limited period: Multiple times over one year
- ☐ Ongoing: multiple times over more than one year

12. How many individuals' Personal Information will be collected?

- ☐ 1 - 50
- ☐ 51 – 1,000
- ☐ Over 1,000

13. Have you determined the minimum amount of Personal Information required for the initiative?

- ☐ Yes
- ☐ No

14. How will you reduce the risk of collecting unnecessary Personal Information? (Check all that apply.)

Web orders would require completion of a form designed and provided by Vendor. Currently being updated by vendor for next version – form will be incorporated by vendor.

VIU will limit collection of personal information to only what is needed to complete the transaction (name, address (if items are delivered), contact phone number or email address (depending on preferred method of contact) and payment information.

- ☐ ☒ Design data gathering forms to gather specific information deemed necessary and directly related for the University Initiative
- ☐ ☒ Design data gathering forms with closed-ended questions
- ☐ ☒ Design data gathering forms with minimal open-ended questions
- ☐ Design data gathering forms with drop-down menus
- ☐ The Business Unit will have documented data gathering processes and requirements

15. If the initiative involves a Third Party, have you confirmed with the Third Party what the minimum amount of Personal Information is required by the Third Party?

- ☐ Yes
- ☒ No
- ☐ N/A (No Third Party involved)

16. FIPPA Notice: If you are collecting Personal Information directly from an individual the information is about, FIPPA requires that you provide a collection notice (except in limited circumstances). Please fill in template and remove bold and square brackets.

Vancouver Island University ("VIU") collects, uses, discloses, and retains your Personal Information in accordance with section 26 of the Freedom of Information and Protection of Privacy Act ("FIPPA"), R.S.B.C. 1996, c.165 for the purposes of facilitating the online purchase and delivery of goods from its campus store. If you have any questions about the processing of your Personal Information, please contact the Privacy Office at **fippa@viu.ca**

NOTE: assess and discuss with the Privacy Office to determine whether informed consent or authorization is required for the University Initiative, as outlined below, to include in FIPPA notice.

Consent:

- Disclosure of Personal Information This is getting at whether the information entered by web customers would then be provided to a party outside of VIU. I think you can answer 'no' to this one, assuming orders will be processed/shipped directly from VIU, but if a payment processor would receive any of the personal information, you should include it. (see #20 below).

- Secondary Use of Personal Information You can answer no to this one, as you will not be using the information provided for any purpose other than what you've collected it for.

Authorization:

- Indirect Collection of Personal Information. This refers to VIU collecting information through another collector, which I don't think applies in your case.

Notice will be provided if PIA deems it is required. The notice at #16 should be included on the web form that information is collected from.

PART 3: USE

FIPPA sets out requirements and restrictions related to use of Personal Information, and includes penalties to public bodies and their employees for unauthorized use. This section will help you identify the legal authority for using Personal Information, and ensure that the use of Personal Information is limited to the original purpose for collection.

17. What is the intended use of the Personal Information collected?

~~To support students purchasing items paid for by a sponsor – verification is required~~
~~To support web orders:~~
- ~~To ensure order is not fraudulent~~
- ~~To ensure ordered items are provided/sent to authorized purchaser~~

18. Does your initiative use Personal Information to make decisions that directly affect an individual?

☐ Yes

☒ No (The response is "No" because the question is related to major decisions)

19. Describe the decisions made.

~~To support students purchasing items paid for by a sponsor – verification is required~~
~~To support web orders:~~
- ~~To ensure order is not fraudulent~~
- ~~To ensure ordered items are provided/sent to authorized purchaser~~

Web orders can be cancelled by the payment system if information cannot be validated.
Is this part of this PIA?

20. Who will be using the Personal Information collected by this initiative? (Check all that apply and provide information requested.)

☐ Your department (please name): Ancillary / Campus Store
~~☒~~

☐ Another VIU department (please name):

☒ A Third Party (please list; i.e. vendor; partner): ~~include the name of the payment processor~~
Chase Merchant Services

21. How will you ensure that parties using the Personal Information will use it only for the purposes stated in 17 above? Check all that apply.

☐ Your department: Documented departmental information management practices and
~~☒~~ training related to this initiative

☐ Another VIU department: Documented communications from your department to the other VIU department, setting out use restrictions

☒ A Third Party: Written contract with VIU

22. Will Personal Information collected for this initiative be used for a purpose other than this initiative? (If yes, FIPPA sets out requirements for the "secondary use". Please consult with Privacy Officer if applicable.)

☐ Yes

☒ No

If yes, describe secondary use:

PART 4: STORAGE

23. Is any Personal Information involved in your initiative stored outside of Canada?

☐ Yes

☒ No

24. Where is the Personal Information stored? Please identify applicable geographic locations for primary storage and backups.

[redacted] s. 15(1)(l)

25. Does your initiative involve Sensitive Personal Information? (Any Personal Information can be Sensitive Personal Information in different contexts. Please contact the Privacy Office to discuss.)

Need to discuss

☐ Yes

☒ No

26. Is any of the Sensitive Personal Information stored outside of Canada?

☐ Yes

☒ No

27. Where is the Sensitive Personal Information stored? Please identify applicable geographic locations for primary storage and backups. Type N/A in the cells on the first row if Sensitive Personal Information is not stored outside of Canada as indicated in Question 26.

Name of Third Party	**Name of cloud infrastructure and/or platform provider(s) (if applicable)**	**Where is the Sensitive Personal Information stored (including backups)?**
N/A	N/A	N/A

PART 5: DISCLOSURE

FIPPA sets out requirements and restrictions related to use of Personal Information, and includes penalties to public bodies and their employees for unauthorized disclosure. This section will help you identify the legal authority for disclosing Personal Information, and to ensure that risks related to the disclosure of Personal Information are duly considered.

Complete this section if you are disclosing Sensitive Personal Information to be stored outside of Canada. You may need help from the Privacy Office.

28. Is any Personal Information being disclosed outside of Canada under FIPPA section 33(2)(f) (if the information is made available to the public under an enactment that authorizes or requires the information to be made public?

☐ Yes

☒ No

29. Is any of the Personal Information being disclosed outside of Canada under FIPPA section 33(2)(p) for the purposes of (i)a payment to be made to or by the government or a public body, (ii)authorizing, administering, processing, verifying or cancelling a payment, or (iii)resolving an issue regarding a payment?

☐ Yes

☒ No

☐ ~~The payment processor is out of scope of this PIA~~

From Vendor:

[redacted] s. 21(1); s. 15(1)(l)

Here is a blog post hosted on the PCI Security Standards website with a little more depth; I shared the Cliffs Notes version. https://blog.pcisecuritystandards.org/assessor-viewpoint-point-to-point-encryption-p2pe-solutions

[redacted]

s. 21(1);
s. 15(1)(l)

30. Describe the privacy risks for disclosure of Personal Information outside of Canada.

Use the table to indicate the privacy risks. For each privacy risk you identify, describe the potential impact to individuals or VIU, and describe a privacy risk response that is proportionate to the level of risk posed.

This may include reference to the measures to protect the Sensitive Personal Information (contractual, physical, technical, administrative measures) you outline elsewhere in this PIA. Privacy risks below are examples only; add new rows if necessary.

I don't think any of these apply for this PIA?

Privacy risk	Impact to individuals or VIU (or VIU employees)	Risk response
Unauthorized collection of PI by VIU employees		
Unauthorized use of PI by VIU employees		
Unauthorized disclosure of PI by VIU employees		
Unauthorized collection of PI by Third Party/ies		
Unauthorized use of PI by Third Party/ies		
Unauthorized disclosure of PI by Third Party/ies		

This content is from previous PIA

Privacy risk	Impact to individuals or VIU (or VIU employees)	Risk response
Unauthorized collection of PI by VIU employees	Data incident or breach	Security/log-in access and tracking to limit employees with access and time/date track use.
Unauthorized use of PI by VIU employees	Data incident or breach	Reporting by any VIU community member of privacy concerns; privacy breach management protocol; human resources conduct investigaitons.
Unauthorized disclosure of PI by VIU employees	Data incident or breach	Reporting by any VIU community member of privacy concerns; privacy breach management protocol; human resources conduct investigaitons.

PART 6: PROTECTION

In Part 6 you will share information about the privacy aspect of securing Personal Information. People, organizations or governments outside of your initiative should not be able to access the Personal Information you collect, use, store or disclose. You need to make sure that the Personal Information is safely secured in both physical and technical environments.

31. Does your initiative involve digital tools, databases or information systems?

☒ Yes
☐ No

32. What physical security safeguards are in place to protect Personal Information in this initiative?

Identify the elements of physical security that protect where the records for your initiative are stored (Check all that apply. Specify, "Other" if applicable)

Safeguard	At VIU	At Third Party
Restricted access to property (i.e. key or key card access and access limited to authorized employees)	[redacted]	[redacted]
Security monitored building	[redacted]	[redacted]
Locked doors	[redacted]	[redacted]
Locked filing cabinets – used for sponsor information	[redacted]	[redacted]
Chain of custody process	[redacted]	[redacted]
"Clean desk" practices	[redacted]	[redacted]
Other:	[redacted]	[redacted]

s. 15(1)(l)

33. What technical security safeguards are in place to protect Personal Information in this initiative?

Describe the elements of technical security that protect where the records for your initiative are stored (e.g. secure passwords, encryption, firewalls, etc.) (More options on the following page)

[redacted]

May require vendor input

Safeguard	At VIU	At Third Party
Authentication control: Strong Password Management	[redacted]	[redacted]
Authentication control: Multi Factor Authentication ("MFA")	[redacted]	[redacted]
Role-based access	[redacted]	[redacted]
Encrypted in transit	[redacted]	[redacted]
Encrypted at rest	[redacted]	[redacted]
Isolation Control: Application	[redacted]	[redacted]
Isolation Control: Network	[redacted]	[redacted]
Isolation Control: Database	[redacted]	[redacted]

s. 15(1)(l)

Vulnerability Scan	[redacted]	[redacted]
Vulnerability Penetration Testing	[redacted]	[redacted]
Configuration Management	[redacted]	[redacted]
Patch Management	[redacted]	[redacted]
Technical control: Perimeter firewalls	[redacted]	[redacted]
Technical control: Web application firewalls	[redacted]	[redacted]
Technical control: Distributed denial of service	[redacted]	[redacted]
Technical control: Intrusion prevention systems to control traffic flow	[redacted]	[redacted]

s. 15(1)(l)

34. What administrative safeguards are in place to protect Personal Information?

Describe the elements of administrative security that protect where the records for your initiative are stored (e.g. aliasing, aggregation, policies/procedures, standards of practice, etc.)

Safeguard	At VIU	At Third Party
Agreement/Contract	[redacted]	[redacted]
Privacy/Data Protection Policy	[redacted]	[redacted]
Documented business practices and processes for proper collection and management of Personal Information	[redacted]	[redacted]
Privacy training specific to the Initiative	[redacted]	[redacted]
Staff Security Awareness Training	[redacted]	[redacted]
Dedicated Information Security Staffing	[redacted]	[redacted]
Information Security Policy	[redacted]	[redacted]
Vendor Third Party Compliance and Certifications (i.e. ISO, SOC Type 2, CSA)	[redacted]	[redacted]
Security Incident Response Plan	[redacted]	[redacted]

s. 15(1)(l)

35. If the initiative involves a Third Party, please indicate what type of Agreement governs the relationship between VIU and the Third Party. Please select one.

- ☐ VIU's GSA (negotiated Agreement between VIU and the Third Party)
- ☐ Vendor's Agreement (negotiated Agreement between VIU and the Third Party)
- ☐ Online "Terms of Service" or "Terms of Use" (often non-negotiable)
- ☐ Memorandum of Understanding/Memorandum of Agreement ("MOU"/"MOA")
- ☒ Other (specify): Agreement between ~~PrismRBS~~ **Chase** Merchant Services and VIU. [redacted]
- ☐ No Agreement

s. 21(1)

36. If the initiative involves a Third Party, does an End User License Agreement ("EULA") apply to the individuals whose Personal Information is involved?

- ☐ Yes
- ☒ No

37. The Privacy Officer will need to review all draft/proposed Contracts/Agreements (and related materials, i.e. contract appendices/schedules; Third Party privacy policies or online terms and conditions, if any) involved in the initiative. Have you ensured these have been provided? Check only one.

- ☒ Yes
- ☐ No
- ☐ N/A (i.e. no Third Party involved in Initiative)

38. Where are the privacy related terms referenced in the contract or agreement if applicable? (Check all that apply)

☒ From Vendor's Standard Agreement

3.3 Customer Data Protection Policies. To the extent that Merchant operates an electronic commerce website through which Transaction Data is generated, in addition to any requirements otherwise set forth in this Agreement, Merchant shall display the following on its website: (a) its Customer data privacy policy; (b) a description of its security capabilities and policy for transmission of Payment Instrument Information; and (c) the address of Merchant's fixed place of business (regardless of website or server locations).
Furthermore, Merchant must offer its Customers a data protection method such as 3-D Secure or Transport Layer Security (TLS).

~~In the body of the contract or agreement~~

~~From Jaret Hoeppner, Contract Specialist~~

[redacted] s. 21(1)

[redacted]

[redacted]

[redacted]

~~Overview~~

[redacted]

s. 21(1)

~~Our support team maintains an account on all systems and applications for the purposes~~

[redacted]

[redacted] s. 21(1)

- ☒ Third Party will be asked to sign VIU's Personal Information Management Schedule
- ☒ Third Party will be asked to sign VIU's Data Security Schedule
- ☒ End user license agreement
- ☐ In a separate Information Sharing Agreement
- ☐ The privacy related terms have not been negotiated yet
- ☐ There are no privacy related terms in the contract or agreement (or related documentation)
- ☐ There is no contract or agreement for this initiative

39. Controlling and tracking access

Review each strategy below that describes how to limit or restrict who can access Personal Information and how to keep track of who has accessed Personal Information in the past. Check all that apply. Specify "Other" if applicable.

- [redacted] Managed role-based access to Personal Information for VIU employees
- [redacted] Managed role-based access to Personal Information for Third Party
- [redacted] Third Party access is time limited for installing, implementing, maintaining, repairing, troubleshooting or upgrading an electronic system — s. 15(1)(l)
- [redacted] Third Party access escorted by authorized VIU employee
- [redacted] Audit logs at VIU
- [redacted] Audit logs from Third Party
- ☐ Other: (*fill in details*)

40. What additional controls are in place to track and prevent unauthorized access to Sensitive Personal Information?

PART 7: ACCURACY AND CORRECTION

In Part 7 you will demonstrate that you will make a reasonable effort to ensure the Personal Information that you have on file is accurate and complete. FIPPA section 28 states that a public body must make every reasonable effort to ensure that an individual's Personal Information is accurate and complete. FIPPA gives an individual the right to request correction of errors or omissions to their Personal Information.

41. How will VIU ensure that the Personal Information is accurate and complete? (Check all that apply)

- ☒ Individuals input their own Personal Information (web orders only)
- ☒ Individuals update their own Personal Information (web orders only)
- ☒ Employee verifies that information is accurate and complete before processing
- ☒ Documented processes to ensure accurate and complete data entry and maintenance
- ☐ The Third Party manages the accuracy and completeness of Personal Information under the direction of VIU
- ☐ Software or service uses automated processes to enter and manage Personal Information
- ☐ Other: (*fill in details*)
- ☐ Other: (*fill in details*)

42. Is there a documented process in place to correct Personal Information?

- ☒ Yes
- ☐ No (plan to put one in place)

43. Sometimes it Is not possible to correct the Personal Information. FIPPA requires a process to make a note on the record about the request for correction if it isn't possible to correct the record itself. Is there a documented process in place to annotate the record?

No Personal Information will be collected by VIU during payment processing

- ☐ Yes
- ☐ No
- ☒ N/A (corrections always possible)

44. If there a request for correction from an individual and VIU or the service provider disclosed that individual's Personal Information in the last year, FIPPA requires that VIU or the service provider provide the applicable other public body or Third Party about the request for correction. Will VIU or the service provider ensure that these notifications are done when necessary?

~~Yes~~

I don't think this applies?

- ☐ VIU will forward correction notifications
- ☐ Third Party will forward correction notifications
- ☐ VIU and Third Party will split responsibility based on who was authorized to disclose Personal Information to third parties before a correction request was made.

PART 8: RETENTION AND DISPOSITION

FIPPA requires that public bodies keep Personal Information for a minimum of one year after it is used to make a decision.

45. How you will ensure the information will be kept for a minimum of one year after it is used to make a decision that directly affects an individual?

~~VIU will be able to set the parameters for this~~
N/A

46. How long will VIU need to retain the records containing Personal Information? If there are different retention timelines for different types of records, please state each retention timeline based on record type.

N/A
~~VIU is developing a records management and retention system pursuant to which all records will be kept for the minimum period specified.~~

47. How long will the Third Party need to retain the records containing Personal Information? If there are different retention timelines for different types of records, please state each retention timeline based on record type.

N/A
~~VIU can set the parameters for this, base on VIU requirements.~~

48. How will you ensure that the records containing Personal Information are disposed of in accordance with the retention schedule noted in questions above?

N/A
~~VIU can set the parameters for this, base on VIU requirements~~.

49. What methods will be used to dispose of Personal Information following retention period? (Check all that apply.)

- ☐ VIU Business Unit shredding on campus
- ☐~~☒~~ VIU contracted shredding service provider
- ☐~~☒~~ VIU deletion of electronic record(s) – will set parameters with vendor system
- ☐ Service Provider shredding/deletion of record(s) under VIU contract
- ☐ Service Provider shredding/deletion of record(s) under VIU written instruction
- ☐ Other (explain):
- ☐ Other (explain):

PART 9: INFORMATION FLOW

50. Complete the Information Flow Table

Use column 1 to describe the way Personal Information moves through your initiative step by step. Describe the steps as if you were explaining it to someone who does not know about your initiative.

Use column 2 to identify whether the action in column 1 is a collection, use or disclosure of Personal Information.

The Privacy Officer will complete column 3 to identify the legal authority you have for the collection, use or disclosure.
We need to review this section

Information Management Steps	**Collection, use or disclosure**	**FIPPA and other legal authorities**
Step 1: online shopper enters PI or store cashier enters PI for select transactions (rentals, serialized merchandise)	Collection	s. 26
Step 2: Merch is associated with customer for transaction (returns, exchanges, warranty retrieval)	Use	ss. 26/27
Step 3: Transaction receipt is generated and shared with customer	Use	ss. 26/27
Step 4:		

Optional: Insert a drawing or flow diagram here or in an appendix if you think it will help to explain how each different part is connected.

PART 10: TRAINING

51. Identify which of the following activities all employees and Third Party (as applicable), will be trained on when collecting and managing the Personal Information for the University Initiative.

~~The following responses are specific to Student Sponsorship accounts, which is a small subset of purchase activity.~~

~~There is a VIU wide training program in development now – so it will be. Until then, training is ad hoc on request to the privacy office.~~

- ☐ ~~☒~~ Collection: Limit the collection to only what is demonstrably necessary
- ☐ ~~☒~~ Use: Use the Personal Information only for the purpose for which it was originally collected
- ☐ ~~☒~~ Access: Only authorized employees (and, where applicable, service providers) may access the Personal Information
- ☐ ~~☒~~ Disclosure: Not to disclose the Personal Information inside or outside VIU unless authorized under FIPPA
- ☐ ~~☒~~ Storage: To store the Personal Information only in VIU-provided or approved storage locations and not to store unnecessarily in multiple locations
- ☐ ~~☒~~ Retention: to keep the Personal Information for a minimum of one year – with longer retention periods only when necessary
- ☐ ~~☒~~ Disposal: To dispose, when applicable, in a secure method that renders the Personal Information permanently irretrievable

PART 11: PERSONAL INFORMATION BANKS

Please provide information about whether your initiative will involve a Personal Information Bank.

52. Will your initiative result in a Personal Information Bank ("PIB")? A PIB is a collection of Personal Information searchable by name or unique identifier. If yes, please complete the table below. If more than one PIB will result, copy and paste an additional copy of the table below and fill out a separate table for each PIB.

☐ Yes
☒ No

Title	
Location	
Personal Information Types	
Categories of Individuals Included	
Collection Authority	
Purpose of Personal Information	
Categories of Persons Managing Information	

PART 12: OIPC REVIEW REQUIREMENTS (Privacy Officer to Complete)

53. Is this initiative a data-linking program under FIPPA? If this PIA addresses a data-linking program, this PIA must be submitted to the Office of the Information and Privacy Commissioner.

☐ Yes
☒ No

54. Is this initiative a common or integrated program or activity? Under section FIPPA 69 (5.4), this PIA must be submitted to the Office of the Information and Privacy Commissioner.

☐ Yes
☒ No

PART 13: PRIVACY OFFICE(R) COMMENTS

This PIA is based on a review of the material provided to the Privacy Office(r) as of **[enter date]**. If, in future, any substantive changes are made to the scope of this PIA, the public body will have to complete a PIA Update and submit it to Privacy Office(r).

[Additional Space for Privacy Officer Comments]

PART 14: SIGNATURES

Privacy Office Signature

This PIA is based on a review of the material provided to the Privacy Office as of the date in Part 13 Privacy Officer Comments above.

Name and Title	Signature	Date signed

Stakeholder Signatures

This PIA accurately documents the data elements and information flow at the time of signing. If there are any changes to the overall initiative, including to the way Personal Information is collected, used, stored or disclosed, the Business Unit will engage with the Privacy Office and if necessary, complete a PIA update.

By signing where required below, the signatories acknowledge and confirm their declarations as noted.

INITIATIVE LEAD (PIA Drafter)

Name and Title	Signature	Date signed

Declaration of Initiative Lead: I confirm that I understand the privacy impacts of this University Initiative and am committed to my FIPPA obligations set out herein relative to the collection and management of Personal Information involved in the initiative. If there are any changes to the initiative, including to the way Personal Information is collected, used, stored or disclosed, I understand that the Business Unit will need to engage with the Privacy Office and if necessary, complete a PIA update. I will establish business practices and processes for proper collection and management of Personal Information and ensure these are documented and followed. I will ensure employees are trained on and able to comply with their obligations under FIPPA; related University policies and procedures; and VIU Privacy Advice, Guidance, and Guidelines relative to this initiative.

DEAN/DIRECTOR

Name and Title	Signature	Date signed

Declaration of Dean/Director: I confirm that I have reviewed this PIA and I acknowledge the residual privacy risks identified. I support the Business Unit by providing required resources to comply with FIPPA and related University policies and procedures; and VIU Privacy Advice, Guidance, and Guidelines relative to this initiative.

INFORMATION SECURITY - Required only when University Initiative involves Information Security

Name and Title	Signature	Date signed

Declaration of Information Security: I confirm that I am satisfied that the Information Security safeguards employed in this University Initiative meet reasonable requirements commensurate with the amount or sensitivity of the Personal Information or VIU business information described in this PIA.

INFORMATION TECHNOLOGY – Required when University Initiative involves use of VIU IT systems (including Teaching and Learning or Library) or integration of Third Party technology with VIU IT systems.

Name and Title	Signature	Date signed

Declaration of Information Technology: I confirm that I understand and approve of the proposed use-case of VIU IT systems described in this PIA, where applicable. I understand and approve of the Third Party's integration with VIU's IT systems for the University Initiative described in this PIA, where applicable.

HEAD OF THE PUBLIC BODY OR DESIGNATE UNDER FIPPA

Required only if Personal Information is involved in the initiative as indicated in Question 8.

Name and Title	Signature	Date signed

Declaration of Head of Public Body or Designate: I affirm that I have reviewed this PIA and accept the residual privacy risks identified for this University Initiative. I confirm that this PIA has been completed in accordance with FIPPA.