Privacy Impact Assessment for:

Agreement on Audit Services with BDO Canada LLP

Initiative:	BDO Canada Financial Audit Services
Department or Service Area Name:	VIU Financial Services

Part 1 – General Information and Overview

1.1 What is the Initiative?

Describe your initiative in enough detail that a reader who knows nothing about your work will understand the purpose of your initiative and who your partners and other stakeholders are. Describe what you're doing, how it works, who is involved and when or how long your initiative runs.

The initiative involves contracting BDO Canada LLP (BDO), an independent audit firm, to perform audit services for the VIU and VIU Foundation. The purpose of the initiative is to ensure the financial statements and related records of VIU are audited for accuracy and compliance. BDO will access online VIU's accounting systems, records, and senior administrators to gather necessary information for the audit. The initiative runs annually starting from Q3 of 2024 and ending on July 31, 2027 with a possibility of extension till July 31, 2029 with BDO providing various reports to the governing boards and committees.

1.2. What is the scope of the PIA?

Your initiative might be part of a larger one or might be rolled out in phases. What part of the initiative is covered by this PIA? What is out of scope of this PIA?

The scope of this PIA covers the collection, use, and storage of personal and financial information accessed during the audit process performed by BDO. This PIA addresses the security, confidentiality, and privacy protection measures in place for the duration of the audit. Out of scope are other unrelated services provided by BDO to different clients or for different purposes.

1.3. Are there any related Privacy Impact Assessments?

Please indicate if this an update on an existing PIA or an additional module that was not covered in the original PIA.

This PIA is not an update on an existing PIA but a new assessment specific to the audit services Agreement with BDO. Our previous external auditors were KPMG up to the end of fiscal 2023-24.

1.4. What are the data or information elements involved in your initiative?

In the table below, please list all the elements of information or data that you might collect, use, store, disclose or access as part of your initiative. If your initiative involves large quantities of information or datasets, you can list categories or other groupings of personal information in an appendix.

Information Type	Information Collected
Personal Information	**From Students:** students records, including names, DOB, home address, student residence, phone number, gender, citizenship, photo, credit card info, fees and payments **From Third Parties:** Contractors' and Customers' names, home/business addresses, email addresses, bank information, fees **From VIU Employees:** payroll records, including names, DOB, job titles, employee numbers, SIN, salaries, email addresses, diversity identity census if shared by employee
Contact details	**From Students:** phone number, address **From Third Parties:** Suppliers' records **From VIU Employees:** work phone numbers, office locations, home addresses
Account information	Bank information.
Commercial information	Financial records, audit reports, management letters

1.4a. Did you list personal information in question 1.4?

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.

Examples of Personal Information	
• Name, age, sex, weight, height • Home address, phone number • Race, ethnic origin, sexual orientation • Medical information • Health history • Number or symbol assigned to the individual • Income, purchases and spending habits • Blood type, DNA code, fingerprints	• Marital or family status • Religion • Education • Financial information • Criminal information • Employment information • Personal views or opinions, except if they are about someone else

- If yes, go to Part 2
- If no, answer question 1.5 and submit questions 1 to 1.5 to privacy.officer@viu.ca. You do not need to complete the rest of the PIA template.

Yes.

1.5. How will you reduce the risk of unintentionally collecting personal information?

Some initiatives that do not require personal information are at risk of collecting personal information inadvertently, which could result in an information incident.

Click or tap here to enter text.

Part 2 – Collection, Use, and Disclosure

This section will help you identify the legal authority for collecting, using, and disclosing personal information, and confirm that all personal information elements are necessary for the purpose of the initiative.

2.1 Four point "Necessity Test" for the collection, use, and disclosure of Personal Information.

To determine if the Personal Information from your initiative meets the necessity threshold, apply the following four-point test to each element of PI from 1.4 above. Note that each element of PI must meet all four points of the test.

Four point "necessity test" for collecting personal information (OIPC Canada, 2016).

1. The information is rationally connected and demonstrably necessary to an operating program or activity
2. The information is likely to be effective in meeting the objectives of the program or activity
3. There are no other less privacy-invasive ways to effectively achieve the objectives of the program or activity
4. The loss of privacy is proportional to the objectives of the program or activity

Personal Information element	Does it meet all four points of the necessity threshold?	Reasons for keeping or excluding from initiative
From Students: students records, including names, DOB, home address, student residence, phone number, gender, citizenship, photo, credit card info, fees and payments	Yes	Required for Auditor to complete audit services.
From Third Parties: Contractors' names, email addresses, fees	Yes	Required for Auditor to complete audit services.
From VIU Employees: payroll records, including names, DOB, job titles, employee numbers, SIN, salaries, email addresses, diversity identity census if shared by employee	Yes	Required for Auditor to complete audit services.

2.2 Personal Information Flow Diagram and/or Personal Information Flow Table

In the table below, list the personal information from question 1.4. Think about how each element of information flows through your project. Your Privacy Officer can help you figure out whether each step is a collection, use, or disclosure, and whether you have the legal authority for the way you're working with the information. Alternatively, you can attach a flow diagram to this PIA. Add rows as necessary.

	Describe the way personal information moves through your initiative step by step as if you were explaining it to someone who does not know about your initiative.	**(Collection, Use or Disclosure)**	**FIPPA or other legal authority**
E.g.	*E.g., Student email, password, and IP address collected by software platform for account creation.*	*Collection*	*FIPPA 26(c) "info relates to and is necessary for a program or activity"*
1.	From Students: students records, including names, DOB, home address, student residence, phone number, gender, citizenship, photo, credit card info, fees and payments	Disclosure	FIPPA 33 (2)(s) "to the auditor general or a prescribed person or body for audit purposes"
2.	From Third Parties: Contractors' names, email addresses, fees	Disclosure	FIPPA 33 (2)(s) "to the auditor general or a prescribed person or body for audit purposes"
3.	From VIU Employees: payroll records, including names, DOB, job titles, employee numbers, SIN, salaries, email addresses, diversity identity census if shared by employee	Disclosure	FIPPA 33 (2)(s) "to the auditor general or a prescribed person or body for audit purposes"
6.			

2.2 Risk Mitigation Table

Thinking through the information flow, identify where there are risks for privacy incidents or data breaches. For each risk, identify a mitigation strategy, as well as the likelihood of an incident, and level of impact or harm if people's information were breached.

Risk Mitigation Table				
	Risk	**Mitigation Strategy**	**Likelihood**	**Impact/harm**
1	Unauthorized access to personal information	The Agreement stipulates that BDO will ensure that confidentiality of information is maintained. Based on proposal from BDO "We treat all client records and data carefully. Client information is only accessible to those working on the job. BDO controls this access via: 1. User access based on their stated roles 2. Formal provisioning processes throughout the user access lifecycle (new user, leaving user, extended leave, job transfer). 3. A mixture of appropriate logical and physical access controls (such as Obtaining authorization for provisioning; Ensuring that the level of access granted is appropriate for requirements and considers the concept of least privileges and segregation of duties; Ensuring that rights are not activated prior to approval; Maintaining a central record of rights granted; Ensuring that proper change of responsibility processes are implemented	Low	High

		4. User responsibilities (Passwords, awareness training, physically securing assets assigned to them) 5. Network access control (Local access, remote access, network services) Our policies over maintenance and destruction of paper and electronic files are set to maximize protection, such as: • Client files are required to be saved into the network and not a hard drive or local drive, and where not possible, they must be uploaded to network as soon as possible and deleted from hard drive • Policies against the use of removable media unless required for services • Paper copies and files required to be shredded or incinerated • Electronic media, including hard drives, tape cartridges and usb must be overwritten a minimum of 3 times prior to physical destruction, which is carried out by an authorized third party with certificates of destruction provided and retained. • Retention Policy lists period of retention – see details in Section 6.3. Finally, identifiable client information is not shared for research or other purposes with		

		anyone inside or outside of the firm. We respect the privacy of our clients."		
2	Data breaches during transmission	Use encryption for data in transit and at rest. Encryption Standards used are TLS 1.2 for encryption in transit and AES 256 for encryption at rest.	Low	High
3	Data breach of BDO files	BDO breach protocol details: Personal Data breaches are required by policy to be reported to BDO's Privacy office as soon as possible, where it is determined if reporting is required by contract or law or both. Security breaches are required to be reported to Infosec as soon as possible. Personnel are trained and instructed to report as soon as possible. Breach response classifies the severity of the incident on a variety of factors and activates a broader incident response team. BDO personnel on the broader response team receive annual training.	Med	High
4				
5				

2.3. Collection or Privacy Notice

If you are collecting personal information directly from an individual the information is about, FIPPA requires that you provide a collection notice, also known as a privacy notification.

A collection notice must contain the following elements:

- The legal authority and section under FIPPA under which you are collecting personal information.
- The purpose for which you are collecting the personal information and how it will be used.
- The contact information of an employee or officer at VIU who can answer questions about the collection of personal information.

Contact the privacy office for a collection/privacy notice template.

If applicable, paste your privacy notice here.

Part 3: Storing Personal Information

3.1. Is any personal information being stored outside of Canada?

If you're storing personal information outside of Canada, identify the sensitivity of the personal information and where and how it will be stored.

No.

3.1.1. Where is the personal information stored?

Personal information is stored on secure servers in Canada as part of the BDO's cloud-based storage solution. Click or tap here to enter text.
Storage provided - MS Azure

3.2. Does your initiative involve sensitive personal information?

Examples of sensitive personal information include personal health information, genetic and biometric data, personal finances, geolocation data, criminal records, counselling records, HR records, payroll records, racial or ethnic origin, sexual orientation, religious, philosophical, or political beliefs, etc.

Yes, financial and payroll records.

If **yes**, please complete **Part 4**: Assessment for Disclosures of Sensitive Personal Information.

If **no**, skip to **Part 5**: Security of Personal Information

Part 4: Assessment for Disclosures of Sensitive Personal Information

Complete this section if you are disclosing sensitive personal information. You may need help from your organization's Privacy Officer.

4.1. Is the sensitive personal information stored by a service provider?

Yes.

If yes, fill out the table below, then go to question 4.3. If no, continue to question 5.

Information about Service Provider

Name of service provider	Name of cloud infrastructure and/or platform provider(s)	Where is the sensitive personal information stored (including backups)?
Microsoft		Secure global portal, with local storage in Canada
Other service providers		Secure global portal, with local storage in Canada

4.2. Provide details on the disclosure, including where and how the personal information is stored.

Answer this if question 4.1 does not apply. Be specific about where and how the information is being stored.

Click or tap here to enter text.

4.3. Is there a contract that includes privacy-related terms?

If there is a contract with the provider, please describe any privacy-related terms in the contract, or attach the privacy schedule.

VIU's Service Agreement includes the following provisions on confidentiality:
" The Contractor must treat as confidential all information in the Material and all other information accessed or obtained by the Contractor or a Subcontractor (whether verbally, electronically or otherwise) as a result of this Agreement, and not permit its disclosure or use without VIU's prior written consent except:
(a) as required to perform the Contractor's obligations under this Agreement, or as expressly permitted by this Agreement, or to comply with applicable laws;
(b) if it is information that is generally known to the public other than as result of a breach of this Agreement; or
(c) if it is information in any Incorporated Material."

"Staff of the Auditor will ensure that confidentiality of information obtained, because of their involvement with the audit, is maintained."

"3. The Contractor must not permit a Services Worker who is an employee or volunteer of the Contractor to have access to Sensitive Information unless the Services Worker has first entered into a confidentiality agreement with the Contractor to keep Sensitive Information confidential on substantially similar terms as those that apply to the Contractor under the Agreement."

BDO has strategic partnerships with Microsoft and other service providers and utilizes contractual or

other means to require service providers to protect the confidentiality and integrity of personal information entrusted to them.

Part 5: Security of Personal Information

Section 30 of FIPPA imposes a duty on the public body to prevent unauthorized access to Personal Information both internally and with any contracted third parties. As such, we need to make sure that personal information is safely secured in both physical and technical environments. **For each item in this section, please describe the security measures for both the service provider and for VIU internally**.

5.1. Please describe the physical security measures related to the initiative (if applicable).

For example, physical security measures may include: the security environment of vendor's data centres; storing records containing PI in locked storage rooms, offices, and/or filing cabinets with controls over distributions of keys/access; locked workstations that do not permit others to view your screen (including when working remotely, etc.

VIU information will be only accessible to those working on the job. BDO's policies over maintenance and destruction of paper and electronic files are set to maximize protection.

5.2. Please describe the technical security measures related to the initiative (if applicable).

E.g. Encryption standard for data in transit and data at rest; firewalls, strong passwords; MFA; encrypted documents, etc.

BDO will have user credentials with access to VIU ERP with 'read only' AVP-FINANCE role access. VIU will upload additional information on BDO's portal which includes multi-factor authentication, DocuSign, data storage encryption, secure document exchange, and audit logging. Docusign is an application that is used to exchange signatures securely.

5.3 Tracking Access / Access Controls. In this section, you will describe how the unit will minimize the risk of unauthorized access to Personal Information.

5.3.1. FIPPA section 30 requires public bodies to manage access to PI based on the principle of "need to know" – that users may only access information that is necessary to do their job. This is frequently accomplished by assigning role-based access controls (RBAC), and by establishing a security matrix that describes which positions/roles are permitted to access specific types or groups of Personal Information. Access to personal information should only be permitted to those who demonstrate their right of access on the security access chart. Please describe how access controls work in the department, or with this initiative.

From BDO's side, VIU information will be only accessible to those working on the job.

5.3.2 How will you know if sensitive personal information is accessed, including access by service providers? This should include a description of what information is available through logs.

VIU's ERP does not have a functionality to log the access to information. ERP can log certain reports ran by the user and stores this information for 30 days.

5.3.3 Please describe any access controls and/or ways in which you will limit or restrict unauthorized changes (such as additions or deletions) to personal information.

BDO will have a 'read only' access to ERP.

5.4 What controls does the provider have in place to prevent unauthorized access to sensitive personal information?

Describe technical, administrative, and/or policy measures in place to protect PI. If using a cloud-based service provider, include a description of controls in each layer of the stack: software level, platform level, infrastructure level.

As per BDO, they use physical, technical, and organizational security measures that are consistent with standards in the accountancy and professional services industry. These security measures are designed to protect the confidentiality and integrity of personal information in their custody. They use contractual or other means to require our service providers to protect the confidentiality and integrity of personal information entrusted to them. Please see information security management sheet: BDO Canada ISO Controls Overview 1.6.pdf

Part 6: Accuracy/Correction/Retention of Personal Information

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. In this section, you will demonstrate how you intend to keep personal information on file accurate and complete.

6.1 How is an individual's information updated or corrected?

FIPPA section 29 states that a person can ask you to correct their personal information in your custody or control. If it is not possible to update or correct (for physical, procedural or other reasons) it must be noted on the record. **Please explain how it will be updated or annotated. If personal information will be disclosed to others, how will VIU notify them of the update, correction, or annotation?**

Individuals can request updates or corrections to their personal information through the Privacy Officer. Once updated, the information will be accessible for retrieval to BDO during the next disclosure. I think employees, students would update info in their employee/student accounts. If not updatable, they would ask HR/Registration.

6.2. Does your initiative use personal information to make decisions that directly affect an individual(s?

No.

6.2.1.If you answered "yes" to question 6.2, do you have an information schedule in place related to personal information used to make a decision?

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

Click or tap here to enter text.

6.3. Do you have a records management schedule in place?

How long will you keep the personal information collected? Is there a plan in place for retention and deletion? Please also use this question to note how long it will be stored by the service provider (if applicable).

Yes, personal information is retained for the duration required by law and contractual obligations, then securely deleted. BDO is required by CPA professional regulations to maintain adequate audit files that evidence its procedures and support its conclusions. If PII is required to be retained to support BDO's conclusions, it would form part of BDO's audit file and is retained in accordance with BDO's retention schedules. This can be for as long as the organization is a client + 10 years. See rule 218 of CPA BC Code of Conduct as well as its Guidance in relation to that rule which references a minimum of 10 years.

Part 7 – Personal Information Banks

A personal information bank (PIB) is a collection of personal information searchable by name or unique identifier.

7.1. Will your initiative result in a personal information bank?

No.

If yes, please complete the table below:

Describe the type of information in the bank
Name of main organization involved
Any other ministries, agencies, public bodies or organizations involved

Business contact title and phone number for person responsible for managing the Personal Information Bank

Part 8 – Further Information

8.1. Does the initiative involve systematic disclosures of personal information? If yes, please explain.

Yes, the information will be disclosed on continuous basis.

8.2. Will the information collected be used for research or statistical purposes?

BDO does not share information for research or other purposes with anyone inside or outside of the firm.

Part 9 – Summary and Proponent Responsibility

This section is for Privacy Office recommendations as well as any limitations due to privacy concerns.

Click or tap here to enter text.

Part 10: 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 program area will engage with their Privacy Office and if necessary, complete a PIA update.

Reviewed by	Privacy Officer
Approved by	Director, Procure to Pay
Date:	13-September-2024