Privacy Impact Assessment for:

Orbis

Initiative:	Orbis Outcomes
Department or Service Area Name:	Centre for Experiential Learning and Student Engagement

Part 1 – General **2**

Part 2 – Collection, Use, and Disclosure **8**

Part 3: Storing Personal Information **12**

Part 4: Assessment for Disclosures Outside of Canada **13**

Part 5: Security of Personal Information **15**

Part 6: Accuracy/Correction/Retention of Personal Information **16**

Part 7 – Personal Information Banks **19**

If yes, please complete the table below: **19**

Part 8 – Further Information **20**

Part 9 – Summary and Proponent Responsibility **20**

Part 10: Signatures **21**

Appendix A: Assessments for Data-linking initiatives and Integrated Programs **22**

Part 1 – General

1. What is the Initiative?

What is the initiative:

Orbis Communications Outcome system integration with the Vancouver Island University Student Record System.

Who is leading the initiative and who else is involved, including partners and stakeholders in and outside government:

The Centre for Experiential Learning and Student Engagement (CEL), Student Affairs at VIU is leading this initiative.

The CEL acting as the experts on experiential learning, provide a variety of career and experiential learning services to students, alumni, staff/faculty and external organizations. The CEL is dedicated to student success through work-Integrated Learning (WIL), career services (Career Studio), peer-supported learning (PSL), Office of Co-Curricular Engagement & Learning (OCCEL). Student learning is enhanced when integrated with academic and experiential education. Services offered by the CEL prepare students for transitioning into life after graduation.

The CEL purchases a license from Orbis Communications, an external corporation located in Ontario, Canada, for use of the online Orbis Outcome system platform, and includes the Co-op/Internship and Career Education Modules. . At VIU this Outcome system has been named “Experience Hub.”

Orbis Communications is one of the most trusted experiential learning solution providers for post-secondary institutions in Canada. For nearly 2 decades, their team has empowered the stories of over 100 institutions, 1 million students and 350,000 businesses.

Using data-driven technologies and tailored strategies their systems promote student success by supporting universities, colleges and employers on their quest to meet students with relevant experiential learning and meaningful career opportunities exactly where they are at today, with exactly what they need for success tomorrow.

In 2022 Orbis was acquired by Symplicity.

The Experience Hub supports students by connecting in-class learning with real world experiences and opportunities. It is an integrated solution that provides post-secondary students easy access to experiential learning opportunities.

This online platform offers the quantifying, tracking, and cataloguing all experiential learning offerings into one streamlined, and easily searchable, digital library and from extractable data sets that reveal an in-depth perspective on student engagement, skills, and growth opportunity areas unique to the VIU campus.

By aligning with the Outcome system (Experience Hub), students are given the highest quality and most tailored experiential learning opportunities available in Canada.

As a provider of software to educational institutions across Canada, Orbis Communications understands Canadian regulations surrounding collection and storage of private/personal data and implements a variety of system limits and safeguards to protect user privacy rights and adhere to institutional and governing authority regulations and Canadian laws.

Where will the initiative take place?

This initiative takes place fully online in the Orbis Outcome (Experience Hub) platform.

When will the initiative take place?

VIU has been using this system since 2010. Expansion of integrated fields is taking place now with a projected due date of March 15, 2024. The system will remain in use until such time as VIU discontinues using the system or replaces the system with a different online system.

Why are you doing the initiative?

The Outcome system has been in use at VIU since 2010. Currently the system is integrated with the VIU student record system and integrates the following information: Student name, ID, phone number and address.

At VIU the Experience Hub is currently used by/for:

- Staff/faculty in a variety of decanal areas to manage work-integrated learning program progression, workflows and data associated with their program/courses.
- An online job posting management system that accepts postings from external employers and internal staff/faculty for both on and off-campus employment and work-integrated learning opportunities.
- Academic, immigration, various faculty and other program advisors and service providers for management of student appointment bookings and related communications.
- Event management and event registration and communications.
- External industry partners/employer customer service management and database.

Information collected in the system is used to carry out essential VIU service programs or work related to service areas.

- Access to student personal information beyond student name is limited to VIU staff/faculty. These employees are provided access to the system to carry out their official duties .
- Anonymous data regarding number of participants, citizenship status, program of study, and work-integrated learning data such as area of work and type of host organization is shared with the Provincial and Federal authorities as required.
- External Industry partner/employer contact information is only shared with students at the discretion of the organizational contact when posting a work opportunity to share with students and is accessible to staff/faculty that use the system as an industry partner database in association with the features/services and/or programs described above.
- Staff/faculty contact information is only shared with students at the discretion of the staff/faculty when posting a work opportunity.

Use of the system will be ongoing until VIU and/or The Centre for Experiential Learning and Student Engagement, Student Affairs decides to terminate the license.
In light of the recent expansion of Experience Hub features and capabilities as well as VIU's work at streamlining systems for efficiency, additional departments have now come on-board with and/or are investigating the use of the system for one or more of the system functions listed above. In order to provide a higher quality functioning of the system that will also enable the ability to lock access to various features down by program of study and to increase the efficiency of reporting work-integrated learning statistics and data to the federal and provincial governing authorities, the CEL has requested IT to work with Orbis on increasing the amount of data being integrated from the student record system to include the additional following information: Program of study, gender, whether or not a student is domestic or international, country of citizenship and Indigenous self-declaration.

How will you carry out the initiative? For example,

VIU IT is working collaboratively with the system designers at Orbis Communications to set up the integration of the additional field information.

1a. Is this initiative a data-linking program under FIPPA?

See Appendix A to determine if your project is a data-linking program.

No, this is not considered a data-linking program under FIPPA as described in Appendix A.

1b. Is this initiative a common or integrated program or activity?

See Appendix B to determine if your project is a common or integrated program or activity.

No, this is not a common or integrated program or activity as outlined in Appendix B.

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 use of Orbis Outcome and integration that is currently set-up through the SRS has been in place at VIU since 2010. The initiative of increasing the amount of data integration in the system will be completed all at once as it involves the increase of only a few more fields of data. An estimated date of expanded data integration is March 15, 2024. This PIA covers all of the initiative and all use of the Orbis Outcome system.

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.

While there was an investigation into privacy law/regulation compliance in 2021 when the contract with Orbis Communications was last renewed, we have been told that there is no PIA existing for the original integration of the system. To the CEL department's knowledge, this is the first PIA completed for the Orbis Outcome system.

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 via data transfer:** Name, age, gender, Home address and phone number Citizenship status and country of citizenship Medical information including physical or mental disability Student ID **Personal Information that may be uploaded by students:** Income while on work experiences Education Financial information Employment information Personal views or opinions

	Criminal Information Resumes, cover letters, recommendation letters Transcripts
	From Third Parties: Name Personal views or opinions **From VIU Employees:** Name Personal views or opinions
Contact details	**From Students:** Name, phone number, address, email **From Third Parties:** Organization name, contact information including phone, email, contact name **From VIU Employees:** Name, email, office location
Account information	**Student ID**
Commercial information	**Organization type, size, GST number**

4a. Did you list personal information in question 4? Yes

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.

- If yes, go to Part 2
- If no, answer question 5 and submit questions 1 to 5 to privacy.officer@viu.ca. You do not need to complete the rest of the PIA template.

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.

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.

6. Personal Information Flow Diagram and/or Personal Information Flow Table

In the table below, list the personal information from question four. 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.

	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.	*Type (Collection, Use or Disclosure)*	FIPPA or other legal authority
1.	Student ID, first/middle/last name, phone number, email, address, gender, citizenship and program of study are integrated into the system automatically from VIU SRS when the student logs in the first time.	Disclosure	33.2 (d) for the purpose for which the information was obtained or compiled, or for a use consistent with that purpose within the meaning of section 34 [*definition of consistent purpose*]
2.	Student ID, name, phone number, email, citizenship status and program of study is used for program and/or course eligibility requirements or communication needs.	Use	FIPPA 32 (a) for the purpose for which the information was obtained or compiled,

			or for a use consistent with that purpose;
3.	Student gender, citizenship, and program of study are disclosed anonymously to Provincial and Federal governing authorities for WIL data and funding purposes.	Disclosure	FIPPA 32.2(d)
4.	Student medical information including physical or mental disability, education, financial information, criminal information, employment information is collected during application to VIU programs/courses.	Collect	FIPPA 26(c) "info relates to and is necessary for a program or activity"
5.	Student medical information including physical or mental disability, education, financial information, criminal information, employment information is used to determine student eligibility and/or need during participation in a VIU program/course	Use	FIPPA 32(a)
6.	Student income while on work experiences, employment information, personal views and/or opinions are collected during the WIL experience.	Collection	FIPPA 26(c)
7.	Student income while on work experiences and employment information is disclosed anonymously to Provincial and Federal governing authorities for WIL data and funding purposes.	Disclosure	FIPPA 32.2(d)
8.	Third party names and contact info are collected during account creation	Collection	FIPPA 26(c)
9.	Third party names and contact info are used for communication regarding VIU student employment and employer engagement opportunities	Use	FIPPA 32(a)
10.	Third party names and contact info is disclosed at their discretion when posting a work opportunity.	Disclosure	FIPPA 33.2 (d)
11.	Third party personal views and opinions are collected during WIL feedback surveys at the conclusion of the WIL experience.	Collection	FIPPA 26(c) "info relates to and is necessary for a program or activity"; 26 (e) "the information is necessary for the purposes

			of planning or evaluating a program or activity of a public body"
12.	Third party personal views and opinions collected during WIL feedback surveys at the conclusion of the WIL experience are used by staff/faculty to judge the quality of the experience and performance of the student while on the WIL experience.	Use	FIPPA 32(a)
13.	Third party personal views and opinions collected during WIL feedback are disclosed to the students who worked with the third party during the WIL experience.	Disclosure	FIPPA 33.2 (d)
14.	Staff/faculty name and contact info is submitted by staff/faculty upon account creation.	Collection, Disclosure	FIPPA 26(c); 33.2(d)
15.	Staff/faculty name and contact info is used for contact and communication during the posting and hiring process.	Use	FIPPA 32(a)
16.	Staff/faculty name and contact info is disclosed to students at their discretion when posting work opportunities	Disclosure	FIPPA 33.2(d)

7. Risk Mitigation Table

Thinking through the information flow, identify where there are risks for privacy incidents or information breaches. For each risk, identify a mitigation strategy, as well as the likelihood of an incident, and level of impact on those if their information was breached.

Risk Mitigation Table				
	Risk	Mitigation Strategy	Likelihood	Impact
1	Authorized employees with access violate VIU policies on privacy and provide the information to unauthorized parties	Provide access only to the minimum amount of information required for an authorized user to perform assigned duties related to the information. Ensure that authorized users with access are aware of VIU policies	Low	The level of impact will depend what private information has been released without authorization and to whom it was released.

		regarding use of personal information accessed during performance of duties.		
2	Erroneously granting un-needed access permission to authorized users	Ability to grant permissions is limited to senior system administrators. Administrators must receive permission from supervisor to grant access. Ensure that all users with any level of access are aware of VIU policies regarding use of personal information accessed during performance of duties.	Low	Authorized user has access to information that they did not need access to. Exposure of un-needed private information to authorized user.
3	System breach by external hackers	Ensure all employees in the CEL have taken Secure I.T. Security Awareness Training as well as VIU Privacy Training, both courses available through VIULearn.	Medium	Exposure of private information to unauthorized sources risking identity theft and other criminal activity.
4		Work with Orbis Communications to ensure that they have sufficient online security in place for external servers.		

8. 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.

Part 3: Storing Personal Information

9. 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, no information is being stored outside of Canada.

9a. Where is the personal information stored?

Canadian Outcome data is hosted in Microsoft's Canada Central region located in Toronto. Backups are also geo-replicated to the Canada East region in Montreal.

10. 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 and payroll records, racial or ethnic origin, sexual orientation, religious, philosophical, or political beliefs, etc. **If so, will the sensitive personal information collected be stored outside of Canada?**

Yes it does include sensitive information but **none is stored outside of Canada.**

If **yes**, please complete Part 4: Assessment for Disclosures Outside of Canada.

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

Part 4: Assessment for Disclosures Outside of Canada

Complete this section if you are disclosing sensitive personal information to be stored outside of Canada. You may need help from your organization's Privacy Officer.

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

If yes, fill out the table below, then go to question 13. If no, continue to question 12.

Information about Service Provider		
Name of service provider	Name of cloud infrastructure and/or platform provider(s) (If applicable)	Where is the sensitive personal information stored (including backups)?

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

Answer this if question 11 does not apply. Be specific about where and how the information is being stored.

13. 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.

14. What controls are 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.

15. How will you track access to sensitive personal information?

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.

16. What are the privacy risks for disclosures outside of Canada?

Use the table to indicate the privacy risks, potential impacts, likelihood of occurrence and level of privacy risk. For each privacy risk you identify describe a privacy risk response that is proportionate to the level of risk posed.

Privacy risk	**Impact to individuals**	**Likelihood of unauthorized collection, use, disclosure or storage of the sensitive personal information (low, medium, high)**	**Level of privacy risk (low, medium, high, considering the impact and likelihood)**	**Risk response (This may include contractual mitigations, technical controls, and/or procedural and policy barriers)**	**Is there any outstanding risk? If yes, please describe.**

Part 5: Security of Personal Information

In Part 5, 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.

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

Information collected via the Orbis Outcome system is stored on Microsoft Exchange Servers located within Canada. All servers are hosted in Microsoft Azure and are subject to Microsoft's physical security policies. Security threat and risk assessments are performed at least annually but are internal and cannot be provided to maintain security.

Information regarding the location and security of Microsoft Exchange Servers can be found here: https://www.microsoft.com/en-ca/trust-center/privacy/data-location

Information regarding Microsoft Azure Servers facilities, premises, and physical security can be found here: https://learn.microsoft.com/en-CA/azure/security/fundamentals/physical-security

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

Permissions in the Orbis system are broken down into two categories:

1. Group A: Primary Permission Groups
2. Group B: Secondary Permission Groups.

Primary groups have a certain amount of permission inherently built into them for the role that user is supposed to be completing in the system. These permissions, set by Orbis, cannot be overridden.

There are six different Primary Permission Groups in the system. Depending on your configurations not all of these groups will be necessary in your installation. Primary Groups are configured based on your specific installation requirements.

- Student
- Faculty/Staff
- Employer
- Alumni
- Portal User
- Portal Staff

Secondary Permissions are used to either:
a.) Control visibility and edit access to parts of the site
b.) Provide users with a way of completing a task or action in a module

The permissions that control visibility access to certain parts of the site typically tend to be more influenced by each institution's way of organizing their sites. These additional access permissions are granted to individuals at a level that is the minimum amount of access required to carry out their job duties as related to and within the system.

Orbis Communications parent company Simplicity Data Privacy Regulations and Frameworks information can be found here: https://www.symplicity.com/compliance/privacy/frameworks

19. 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.

Access to make changes to account information is limited to the user/owner of the account and limited staff/faculty who have been granted the rights to amend or delete system account in order to perform their job duties. Granting of these rights/access permissions is at the discretion of the director, Centre for Experiential Learning and Student Engagement. Extensive training and training manuals are provided to guide these users on the management of accounts. Including the process for receiving requests for changes to account information and recording the request on an account note as a confirmation that the account change request was received from an authorized individual. i.e. The account holder or organization that employes the account holder in the case of external employer accounts.

20. Please describe how you track who has access to the personal information.

The system provides a list of system roles and permissions and who has these permissions and roles. System administrators also have access to system logs in which they can view all system activity and accesses.

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.

21. How is an individual's information updated or corrected?

Integrated student information is collected via the student record system. VIU policies and processes for keeping student record information up to date will apply. The CEL has no oversight of the student record system or VIU policies and processes for keeping this information up to date and must rely on the registration/records to fulfill this obligation. If incorrect information is discovered, students will be prompted to make changes in the student record system which will be reflected in the Orbis Outcome system.

Information collected for program/course participation will be governed by VIU policies around retaining/updating information used for academic and service operation purposes and will only be changed, updated or corrected by an authorized VIU authority.

Industry Partner/Employer information is kept up to date by communication with these account holders to confirm that system information is still up to date and accurate. If an industry partner/employer is

non-responsive to communication the account is deactivated until such time as they contact us to confirm up to date an accurate information.

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 annotated. If personal information will be disclosed to others, how will VIU notify them of the update, correction, or annotation?**

Student accounts: Changes to student personal information must be made in the student record to be updated in the system. If a student requests that information in the Orbis Outcome system be updated they will be directed to make the change in their student record. A note will be added to the student account to record the requested change. The account information may be changed manually when requested but until the student record system is changed it will be overwritten by the system integration.

External Employer accounts: Almost all requested changes to employer accounts can be made immediately by an authorized user. A note will be added with the requested change information. If the change cannot be made due to procedural or other reasons, the account will be rendered inactive until such time that the change can be made or, if no history to be kept, will be deleted.

Staff/Faculty accounts: Staff/faculty account info change requests can be made immediately by an authorized user. Outdated accounts with no attached history will be deleted. Outdated accounts with history that is required to be kept will be make inactive to prevent access to the system and a note will be attached to the account detailing why the account was made inactive.

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

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

The information may be used to determine if a student is eligible to receive grant funding, participate in an opportunity/academic program or have completed requirements to receive academic credit or completion notation. Information also provides direction and/or recommended actions to service team members to determine services that need to be provided to students.

22a. If you answered "yes" to question 22, please explain the efforts that will be made to ensure that the personal information is accurate and complete.

Data entered for purposes listed in question 22 is used by the same authorized user that enters the information. Information used in questions 22 is normally collected and entered at the time of use so is expected to be up to date. Accuracy and completeness of information is the responsibility of the user that is entering it for future use. Information that may be subject to changes with time will be confirmed prior to use for decision making purposes that will affect the individual.

23. If you answered "yes" to question 22, do you have an information schedule in place related to personal information used to make a decision?

The information schedule is based on the program or reason that that data is being stored for decision making purposes. I.E Grant funding eligibility will be confirmed and or updated on the schedule related to application for the same. Information used to make a decision will be kept on file for a minimum of one year after it is used to make a decision as required by FIPPA.

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

24. 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).

The information will remain in place for as long as VIU maintains the system license or until such a time that VIU is no longer legally obligated to store that data and has been requested to remove or delete the data. Data used for decision making will be kept for a length of time as prescribed in the VIU policies regarding academic data retention. As this data is stored on external servers, it will remain in place on the external servers until such time that it is removed from our Outcome system. At that time the servers will update stored data to reflect the changes.

A schedule of system maintenance for date upkeep and retention is described in the Orbis Outcome (Experience Hub) user manual created for system administrators.

Student data is kept for an amount of time prescribe by VIU policies
Employer data is kept for the following amount of time:

- Active account – as long that the account is being actively used
- Inactive account – following one year of no use with no historical records account will be deleted from system
- Inactive account – following 5 years of no use with historical records account will be deleted from system

Staff/faculty account is kept for the following amount of time:

- Current VIU employee account – as long user is employed at VIU
- Former VIU employee account – with no historical records account will be deleted from system immediately following departure from VIU employment
- Former VIU employee account –with historical records account will be deleted from system following 5 years of departure from VIU employment

Part 7 – Personal Information Banks

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

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

Yes, the Orbis system functions as a personal information bank for VIU staff/faculty that use the searchable information to carry out their VIU job duties.

If yes, please complete the table below:

Describe the type of information in the bank
Student: Student ID, name, age, gender, home address and phone number, citizenship status and country of citizenship, indigenous self-declaration
External Organizations: Name, Type, Size, website
External Employers: Name, address, email, phone
Staff/faculty: Name, job title, office location, phone number, email

Name of an individual who may be contacted regarding the PIB: Danielle Johnsrude, Director, Centre for Experiential Learning and Student Engagement

Department responsible for the PIB: Centre for Experiential Learning and Student Engagement, Student Affairs.

Part 8 – Further Information

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

Yes, student personal information will be disclosed to authorized staff/faculty users who use the system to complete their job duties. As a student applies to a course or program administered by an authorized user, the students name, student ID, address, email, phone number, program of study, gender and citizenship will be disclosed to users that have been granted access to view this information as required by their job duties.

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

Yes. Some of the information will be used to report anonymous student work-integrated learning numbers to the Provincial Government and anonymous student system usage to other VIU departments. Citizenship and gender will be disclosed but anonymously, not connected to any other identifying information.

Part 9 – Summary and Proponent Responsibility

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

- What data security measures does Orbis have in place to protect the transfer/integration of information from VIU to Orbis servers?
- What personal information does VIU share with employers through the Outcomes platform?
- Do employers see a privacy notification when accessing this information?
- Does VIU share student's information with 3rd party recruiting services through the platform?
- Opt-out/ object to Symplicity/Orbis from using student information for direct marketing purposes. There is a provision for this in the Symplicity Privacy policy by contacting "Data Privacy Requests"
- Consider creating documentation/tracking sheet that lists VIU employee positions and their associated access levels in Outcome system. This could be a spreadsheet that tracks employee, position and access level. Identify manager/admin responsible for assigning/removing access and updating tracking sheet.
- Consider creating documented procedure for removing access from employees who change positions or leave department/VIU. Could be part of document as above.
- Ensure all employees in the CEL have taken Secure I.T. Security Awareness Training as well as VIU Privacy Training, both courses available through VIULearn.

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, Student Engagement and Experiential Learning
Date:	31-May-2024

Appendix A: Assessments for Data-linking initiatives and Integrated Programs

Determine whether this program is a "Data linking Initiative."

In FIPPA, "data linking" and "data-linking initiative" are strictly defined. Answer the following questions to determine whether your initiative qualifies as a "data-linking initiative" under the Act. If you answer "yes" to all 3 questions, your initiative may be a data linking initiative. If so, you will need to comply with specific requirements under the Act related to data-linking initiatives.	
Personal information from one database is linked or combined with personal information from another database;	Yes
The purpose for the linkage is different from those for which the personal information in each database was originally obtained or compiled;	No
The data linking is occurring between either (1) two or more public bodies or (2) one or more public bodies and one or more agencies.	Yes
If you have answered "yes" to all three questions, please contact a PCT Privacy Advisor to discuss the requirements of a data-linking initiative.	

Determine if this program is a "common or integrated program or activity."

In FIPPA, "common or integrated program or activity" is strictly defined. Answer the following questions to determine whether your initiative qualifies as "a common or integrated program or activity" under the Act. If you answer "yes" to all 3 of these questions, you must comply with requirements under the Act for common or integrated programs and activities.	
This initiative involves a program or activity that provides a service (or services);	Yes
Those services are provided through: (a) a public body and at least one other public body or agency working collaboratively to provide that service; or (b) one public body working on behalf of one or more other public bodies or agencies;	No
The common or integrated program/activity is confirmed by written documentation that meets the requirements set out in the FOIPP regulation.	Yes
Please check this box if this program involves a common or integrated program or activity based on your answers to the three questions above.	No