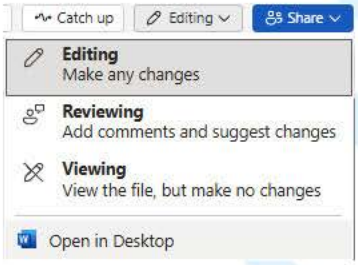
Privacy Impact Assessment for:

VANCOUVER ISLAND UNIVERSITY

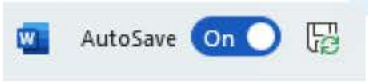
Unit 4

Initiative:	Unit 4
Department or Service Area Name:	Legal Services

Tip: Consider using the Microsoft Word Desktop app for a better experience while completing this form.



Once in desktop, the file should be linked to the online version. Just ensure that the autosave toggle is enabled (upper left side of screen):



VANCOUVER ISLAND UNIVERSITY

Unit 4

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.

Vancouver Island University has engaged Unit 4 ERP platform for managing institutional services including the Human Resources Information System (HRIS) which includes Payroll, as well as the Financial Information System (FIS). This PIA was initiated for a 2025 contract renewal. The initial term of the contract is three years with year-to-year renewal periods after that. Start date is retroactive to June 28, 2025.

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?

This PIA is a general assessment of Unit 4's privacy policies and practices. It does not cover the specific ways that VIU is using the products.

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.

No.

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	Full legal name, addresses, phone numbers, email addresses, DOB, age, spoken language, citizenship, social insurance number, marital status, beneficiary details under benefits, gender, employment information (including: salary, position, pay scale, pay step, employer, personal notes, photos, username, start and end dates of employment; employment

	history at institution); tax information (including employment related tax forms); paystubs; benefits information, performance information, ethnicity/race, union membership, emergency contact details (name, relationship, phone number); bank account info;
Contact details	
Account information: what info is required to set up an account?	
Commercial information	

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

Personal information (PI) 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- see the table below for examples of Personal Information.

Business contact information, in turn, is defined as information to enable an individual at a place of business to be contacted and includes the name, position name or title, as well as business telephone number, address, email or fax number of the individual. BC FIPPA does not protect business contact information.

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 pia@viu.ca. You do not need to complete the rest of the PIA template.

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

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

N/A

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
All PI elements listed in 1.4	Yes	1. To facilitate the VIU employer-employee relationship, including payroll. 2. To manage the finances of the University.

2.2 Does your initiative involve the use of Artificial Intelligence (AI)? If so, please fill out Appendix One: GenAI Analysis Questions

Not currently.

2.3 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 (Privacy Office)**
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.	All information in section 1.4 above is collected by VIU for the purposes of facilitating the employer-employee relationship.	Collection	s. 26(c)
2.	All information from section 1.4 is used by VIU as employer to facilitate employer-employee relationship (for example, to process payroll or approve expenses and absence requests); and by VIU employees in the self-serve portal (for example, to submit vacation requests or timesheets).	Use	s. 32 (a)

3.	In the act of executing employment-related transactions as described above, personal information is disclosed to Unit 4 as the platform/interface provider.	Disclosure	s. 33(2)(d)
4.			
5.			
6.			

2.4 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 VIU employee personal details	Unit 4 staff trained on emerging security threats and issues and are vetted (subject to local laws) prior to employment. VIU employees have access to training on cybersecurity and privacy and are	Med	Med

		encouraged (though not currently required) to take training. VIU employees are subject to policy 22.04: Compliance with BC FIPPA and HR employees must follow 43.10: {Confidentiality of} Personnel Files		
2	Data breach Unit 4 servers	For Unit 4 security overview, see section 5 below. Also, Unit 4 data security policies have been reviewed and vetted by VIU Information Security team. Security Measures (Technical and Organisational) According to section 9: Unit4 Data Processing Policy: Unit4 will notify VIU without undue delay after becoming aware of a personal data breach, providing VIU with sufficient information to enable VIU to meet breach reporting obligations, and at VIU's request will assist in the investigation, mitigation, and remediation of each Personal Data Breach in order to enable VIU to comply with data protection laws.	Low	High
3	Personal data compromised in transit or at rest	Customer data in transit over public networks is protected with TLS 1.2. Transactional data at rest is protected using Transparent Data Encryption (TDE), while non-transactional data and files will be		

		secured by Standard Symmetric Encryption (AES).		
4	Unauthorized acccess			
5				

2.5. 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.

Unit4/VIU ERP data likely stored in Canada but there may be contracted third parties that do not store in Canada.

3.1.1. Where is the personal information stored?

Azure servers in Eastern Canada.

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

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)?
Unit 4	Microsoft Azure	Quebec City and Toronto
*These are the data centers listed on the Unit 4 ERPx Cloud Service Description.		

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.

N/A

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.

Yes: https://info.unit4.com/rs/400-HYB-295/images/Unit4-General-Terms-of-Business-v3.4-April-2025-EN.pdf
See page two, item 7: Data, Privacy and Data Protection
7.1 "Analytics and AI: Essentially states;

- that Unit 4 is entitled to use any VIU data it processes to produce Analytics and to improve/enhance their services by providing info to machine learning mechanisms and by making use of algorithms.
- Unit 4 Analytics made available to a third party will not contain any personal data or identify VIU.
- Unit 4 will not Customer Confidential Information or Personal Data in tooling that allows such data to become part of a publicly searchable database (i.e. Generative AI tooling).

7.2 Privacy and Data Protection: "Each party shall comply with their respective obligations set out in Unit4's Data Processing Policy.

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.

Physical safeguard	VIU	Third Party
Restricted access to property (e.g. key card access)	☒	☒
Security monitoring building	☒	☐
Locked doors	☒	☒
Locked filing cabinets	☒	☒
Locked workstations	☒	☐
Security cameras/ video surveillance systems	☒	☐
Other: Employees and contactors return all Unit4 assets upon termination of employment/contract Records of return maintained.	☒	☒
Other: Media (including hard drives) disposed of securely when no longer required. All sensitive material removed by guaranteed removal software before disposal or physical destruction.	☐	☒

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.

Technical Security Measure	VIU	Third Party
Strong password requirement	☒	☐
Multi-factor authentication (MFA)	☒	☐

Role-based access	☒	☒
Encryption in transit	☒	☒
Encryption at rest	☒	☒
[redacted] s. 15(1)(l)		
Other	☐	☐
Other	☐	☐

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

Unit 4: "Access is strictly limited to only those who require it and is reviewed on a regular basis." https://www.unit4.com/why-choose-unit4/security-privacy

Under Application level security, Unit 4 enables VIU to configure access controls accordingly:

- **User-/role-level permissions** – advanced granular permissions (Read, Write, Update, Delete) can be defined either by user or role and fully managed by VIU.
- **Data-level permissions** – within a defined set of user/role permissions, Unit4 applications allow for granular data filtering.

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.

Unit4 will retain limited back-end access to customer data (by direct database connection). Access by Unit4 shall be strictly limited to activities necessary for installing, implementing, maintaining, repairing, troubleshooting, or upgrading the solution. All access is logged and limited to a small group of Cloud Engineers, Professional Services and Support Consultants.
Access logs are saved in the centralized monitoring solution for 365 days. In case of data breaches, Unit4 can provide the access logs on request.

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.

See Unit4 Security Measures (Technical and Organisational)

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.

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?**

Some data fields can be updated directly by employees in the Unit4 portal; others can be updated by Human Resources by emailing hr@viu.ca.

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

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

Yes. See Data Processing Policy Item 8 **Deletion or Return of Customer Personal Data**: Unit 4 will return the Personal Data at the end of the Provision of the Services relating to Processing and then delete the Personal Data from its systems, or otherwise simply delete the Personal Data without returning a copy to Customer. (All subject to applicable laws).

VIU – see draft Records Classification and Retention Schedule.

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).

- According to Unit 4: *Guide to Contracting with Unit 4*, "Customer data belongs to the customer and determines how it is accessed and used. Unit4 may use this data in an anonymized way for creating analytics (without identifying the customer). Should our relationship with a customer comes to an end, Unit4 will make available a copy of all customer data in agreed format (pg.4)"
- According to section 8 in the Unit 4 Group Data Processing Policy v.1.3: "Unit 4 will, at the choice of the Customer, return the Personal Data at the end of the provision of the Services relating to Processing and then delete the Personal Data from its systems, or otherwise simply delete the Personal Data without returning a copy to the Customer." (unless required otherwise by applicable laws, regulation, court order, etc.). "If no choice has been made by

the Customer within 30 days of the end of the Provision of the Services, Unit4 will automatically delete the personal data."

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?

Yes

If yes, please complete the table below:

Describe the type of information in the bank
VIU personnel employment information (see section 1.4 above for approximation of PI in database).
Name of main organization involved
Unit4
Any other ministries, agencies, public bodies or organizations involved
VIU
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.

No

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

Unit 4 has stated they are entitled to use VIU data for Analytics. See Unit4 General Terms of Business, 7.1 Data Analytics and AI.

Part 9 – Summary and Proponent Responsibility

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

Reference documents:
Guide to Contracting with Unit4
Unit4 Data Processing Policy
Unit4 Details of Processing
Unit4 Business Security Measures
Unit4 Information Security Policy
Unit4 ERPx Cloud Service Description

Part 10: Signatures

VANCOUVER ISLAND UNIVERSITY

Unit 4

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	
Date:	2025-10-07