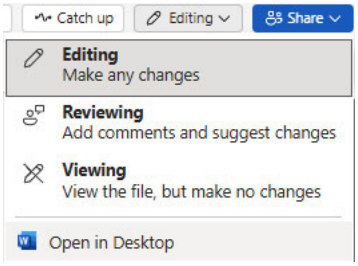
Privacy Impact Assessment for:

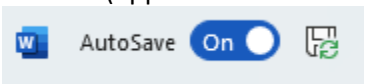
Interceptum Surveys

Initiative:	Interceptum Survey tool for use in VIU Fear & Anxiety Lab
Department or Service Area Name:	Psychology Fear and Anxiety Lab

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

Interceptum Surveys

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 Fear and Anxiety Lab intend to use a Canadian survey platform owned by Acquiro Systems Inc, a Canadian graphic design and software company headquartered in Gatineau, Québec. The platform provides several features including survey design, response collection, survey access, security, data exports, response analysis, Interceptum access, and support. Surveys may be distributed via email links or posted links. The Fear and Anxiety Lab research team, comprised of undergraduate VIU psychology students, and the lab supervisor, Dr. Melanie O'Neill, will be using the survey platform. The Fear and Anxiety lab will pilot Interceptum for one year and then consider whether to adopt the platform for a longer term.

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 covers the use of Interceptum in the Fear and Anxiety Lab only.

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. New PIA (first deployment of Interceptum at VIU). No related PIA.

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	• . Specific demographic questions for surveys vary per survey, but may collect personal information such as age, sex, gender, sexual orientation, race, income, marital status, religion, level of education, medical information, and/or personal views.

	• Contact details for invitations (name, email) [optional] • Survey responses (may include opinions/views) • Technical metadata generated by the platform (e.g., timestamp; IP/log data if enabled)
Contact details	No contact information is collected for participants when completing surveys.
Account information: what info is required to set up an account?	-Credit card information with billing address and phone number -An email account (for the Fear & Anxiety Lab coordinator[s])
Commercial information	N/A

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	
• 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 • IP Address

- 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.

Yes. Specific demographic questions in surveys may ask for age, sex, gender, sexual orientation, race, income, marital status, religion, level of education, medical information, or personal views.

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.

Both online and in-person recruitment explicitly states that this survey is anonymous. The consent forms state that any demographic information is non-mandatory and that participants are free to withdraw their participation at any time.

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
Age	Yes	Used as a control variable. Optional so participants can choose not to answer.
Sex, gender, sexual orientation	Yes. However, depending on the study, it may not be necessary.	Used as a control variable. Optional so participants can choose not to answer.
Race	Yes	Used as a control variable. Optional so participants can choose not to answer.

Income (range)	Yes. However, depending on the study, it may not be necessary.	Used as a control variable. Optional so participants can choose not to answer.
Religion	Yes. However, depending on the study, it may not be necessary.	Used as a control variable. Optional so participants can choose not to answer. Not included in every study.
Level of education	Yes. However, depending on the study, it may not be necessary.	Used as a control variable. Optional so participants can choose not to answer. Not included in every study.
Marital status	Yes. However, depending on the study, it may not be necessary.	Used as a control variable. Optional so participants can choose not to answer. Not included in every study.
Medical information	Yes. Only included when specifically relevant to the study.	Used as a control variable. Optional so participants can choose not to answer. Not included in every study.
Personal Views	Yes.	Used as a control variable. Optional so participants can choose not to answer. Not included in every study. Necessary to obtain feedback, however, questions can be designed to avoid collecting unnecessary Personal Information.
Contact details (optional names, VIU email)	No - Anonymous links are less invasive but there maybe times when surveys are sent to specific cohorts.	Required to send invitations when targeted distribution is needed. Ensures survey reaches correct recipients.

Technical metadata (timestamp, IP if enabled)	Depends on whether provider has option to disable IP collection.	Supports platform functioning.

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

No.

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.	The Lab Coordinator email is collected by the software program for account creation. A username and a password are created for the account.	Collection by Interceptum through their website.	s. 26(c)

2.	A personal credit card with billing address and phone number are entered for the account.	Collection by Interceptum through their website. Use by Interceptum to charge/invoice for the subscription.	s. 26(c)
	***All items below are survey -specific and should be authorized by REB. ***		
	If using distribution list: Invitation emails (optional names and email address) uploaded to Interceptum for distribution	Survey team collects names, emails – uploads/discloses to Interceptum	REB - Consent
	Respondent opens survey link and submits responses; identity not collected unless necessary	Collection	REB- Consent
3.	During surveys, participants are asked to complete non-mandatory demographic questions. Demographic questions in surveys may ask for age, sex, gender, sexual orientation, race, income, marital status, religion, level of education, or medical information.	Collection in Interceptum. Use in SPSS for statistical analysis.	REB - Consent
4.	Personal views may be collected in open-ended questions. Participants are reminded not to include identifying information. Any identifying information will be removed prior to qualitative analysis.	Collection in Interceptum. Use of de-identified open-ended responses for	REB - Consent

		analysis in Microsoft Excel.	
	Authorized survey team/ staff view aggregated reports in Interceptum	Use/Disclosure	REB- Consent
	Suvey team exports results to VIU storage Raw survey data stored on VIU shared drives? SharePoint?	Retention	REB data storage requirements/ FIPPA s. 30 safeguards
	Vendor stores data in AWS Canada (Canada Central – Montreal) with access restricted to authorized personnel. (Data stored until survey team takes active step of deleting from servers).	Retention	REB data storage requirements/ FIPPA s. 30 safeguards
5.	Data will be combined (aggregated) through statistical and qualitative analysis and presented through abstracts and presentation posters, final reports for directed studies and honours projects, and potentially submitted to journals for publication.	Use, Disclosure	REB - Consent

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	Prospective participants may reveal identity on social media recruitment	Anonymity is explicitly mentioned. Comments turned off on posts when websites allow.	Med	Med
2	Account and password shared outside of research team	Lab members are clear on privacy expectations and how to prevent breach of information.	Med	High

		Ensure all members have recent TCPS 2_Core certificates Create Role-based-Access chart and have plan for off-boarding individuals who leave research team or lab.		
3	Demographic questions (sex, age, income, etc.) are asked	These questions are non-mandatory and protected behind a password. Participants are explicitly told that they are allowed to not answer questions or withdraw participation at any time.	Med	Med
4	Personal views may be collected in open-ended questions.	Participants are reminded not to include identifying information. Any identifying information will be removed prior to qualitative analysis.	Low	Med
5	Data will be combined (aggregated) through statistical and qualitative analysis and presented through abstracts and presentation posters, final reports for directed studies and honours projects, and potentially submitted to journals for publication. Risk of re-identification through mosaic effect.	All participant information will be unidentifiable. There will be no risk for personal information to be shared in the process of knowledge mobilization. All participant data will be aggregated and stripped of personal identifiers. Cell counts lower than 10 will be masked in reporting.	Low	Med
	Personal data compromised in transit or at rest on Interceptum servers.	Transport Layer Security (TLS) encryption (also known as HTTPS or SSL) with strong encryption and SSL certificates with 2048 bit keys. We regularly patch our servers when	Low	High

		vulnerabilities related to TSL/SSL connections are disclosed. All security features of AWS data centres		
	Breach of Interceptum servers	Acquiro Systems maintains a policy of full event disclosure for security incidents that affect client data. In the event of any security incident affecting your data, a notification will be sent to your account administrator.	Low	High
	Unauthorized access – Interceptum employees	Employee background checks; signed confidentiality agreements; annual security and privacy training; Role-based-access-controls (RBAC): access to Interceptum servers is restricted to specific individuals and their access is monitored and audited for compliance.	Low	Med
	Unauthorized access (VIU research lab shared drive)	Password protected computers in lab Password protected Interceptum account RBAC list and Off-boarding checklist	Low	Med

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.

We do include a statement on the consent form. However, this likely needs to be updated to include the above elements. We will require a template to update our statement. Here are some sections from the consent form that cover items requested. We do not have the legal authority and section under FIPPA or the contact information for an officer at VIU who can answer questions.

There is no direct benefit to taking part in this study. Participants can take breaks while completing the survey and return to it later. Participants have the right to decline to answer any question they do not wish to answer, and they may withdraw from participation at any time by navigating to the consent form using the "previous" button located at the bottom of the survey.

This study is designed to protect participants' anonymity. No personally identifiable information will be collected at any point. **Please do not include your name or contextual information that might directly or indirectly identify you.** Participants are under no obligation to share information that they do not feel comfortable disclosing and may withdraw consent, alter answers, and skip questions at any time prior to submitting the survey. However, due to the anonymous nature of the data collection, withdrawing will not be possible after the survey is submitted.

Responses to this survey will be stored on Interceptum's database. Interceptum's servers are located in Canada. For more information regarding Interceptum's terms of service, follow the link provided: https://interceptum.com/pa/en/privacy-policy.

All records will be kept strictly confidential. All data collected will be stored electronically on a secured drive at Vancouver Island University. Only the research team and the research supervisor will have access. Consent forms and data collected for the purposes of this study will be kept on the secured drive for the duration of the project, and then deleted from both Interceptum and the drive no later than five years after the study's publication in an academic journal (approximately June, 2031).

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?

Quebec, Canada (check on the specific city)

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)?
Acquiro, Inc.	Amazon AWS	Amazon AWS in the Canada Central Region, Montreal, Quebec

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.

All data collected on Interceptum will only be accessible with SPSS on Vancouver Island University (VIU) servers. Raw data will only be accessible by the principal investigator and Fear and Anxiety Lab members. Data will not be stored outside of VIU's secure computers, for example via cloud-based storages. All unaggregated data with be permanently deleted after completion of the studies.

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.

Interceptum Privacy Policy: https://interceptum.com/pa/en/privacy-policy
Interceptum Security Statement: https://interceptum.com/pa/en/security-statement

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: recorded in/out logs from data centre	☐	☒

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

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

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.

The principal investigator (PI) and the Fear and Anxiety research lab will have access through Vancouver Island University's A-drive.

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.

Access to Interceptum servers is restricted to specific individuals, whose access is monitored and audited for compliance.
All information provided by participants stored on Interceptum are unidentifiable.

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.

Survey results are behind a password protected wall in which only lab members have access on secure computers. See section 5.2 for security controls.

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?**

Personal information will be unable to be updated. Participant information is unidentifiable as responses to questions on the survey platform are anonymous.

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.

No personal information is used that may directly affect an individual.

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).

Describe data retention plan.

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
N/A
Name of main organization involved
Vancouver Island University
Any other ministries, agencies, public bodies or organizations involved
No.
Business contact title and phone number for person responsible for managing the Personal Information Bank
N/A

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?

Yes. For research purposes.

Part 9 – Summary and Proponent Responsibility

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

s. 13(1)

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	VIU Fear and Anxiety Lab program chair
Date:	09-March-2026