VANCOUVER ISLAND UNIVERSITY

Privacy Impact Assessment for:

Border Pass AI

Initiative Title:	Border Pass AI
Department or Service Area:	Office of Future Students

VANCOUVER ISLAND UNIVERSITY

Privacy Impact Assessment for:

Border Pass AI

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.

In response to declining international student enrolments, VIU needs to work harder on retaining, or converting the limited number of applications to VIU into registered VIU students. By partnering with BorderPassAI, VIU will demonstrate a competitive advantage in this marketplace by offering support to our prospective students for the study permit process. A process that has become increasingly difficult and uncertain. BorderPass is an immigration management company that carefully walks students through the study permit application process to make sure that the application that the student submits is a successful one. VIU will not be providing any information to BorderPass. Through communications sent to students, they are invited to access BorderPass and provide BorderPass with the required documents necessary for a study permit application. VIU is not part of the study permit application process. The intent is to purchase BorderPass subscription for our prospective students for 1 year.

The Service will include pre-screening assessment of international applicants as well as study permit review and filing.

The **pre-screening process** is meant to improve the admissions process and enhance the likelihood of approval for those who receive LOAs/PALs, which increases the conversion rate from application to enrollment.
BP also claims to reduce the cost per application to VIU by:

- **Automated screening**: uses BP software tools to automate the initial screening process by filtering out applications that are less likely to meet required criteria, allowing priority for "high conversion candidates."
- **Data**-informed LOA/PALs: leverages admissions and immigration data that will enable VIU to make informed decisions about offering acceptances by focusing on applicants with a higher probability of meeting DLI acceptance criteria and successfully obtaining study permits.

Study Permit Review and Filing:

- Applicant receives study permit application preparation, review, and filing services as well as PAL submission through BP by Canadian Immigration Lawyers;
- Applicants receive pre and post-arrival immigration packages as well as step by step guidance regarding their journey to Canada and the border process.
    - Includes the ability to search and secure accommodations based on their preferences.

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 the PIA is to assess the use of BorderPass for prospective international students.

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	**From Students:** VIU is not collecting new information from students **From Third Parties**: VIU provides a unique URL for BorderPass to students. All information provided by the student to BorderPass is covered by BorderPass's privacy agreements https://www.borderpass.ai/privacy-policy All personal data is extracted from user inputted documents or assessment answers, as required to provide services as needed by IRCC. Personal Data Includes: · Name, age, sex, weight, height · Home address, phone number - country of origin / residence · Health history · Marital or family status · Education information - Past Immigration information · Financial information · Criminal information · Employment information **From VIU Employees: None**

Contact details	**From Students:** Not collecting or providing any student contact information **From Third Parties:** Only a unique URL is shared with students who have applied to VIU through our application process **From VIU Employees:** None
Account information: what info is required to set up an account?	VIU will provide a URL link to prospective students inviting them to use the services of BorderPass.
Commercial information	*None*

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- 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.

Click or tap here to enter text.

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.

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?	Reasons for keeping or excluding from initiative
All details re collection, use and disclosure of personal information can be found here: https://www.borderpass.ai/privacy-policy and in Data Management Policy Package attached	Yes	Required to perform services (filing immigration applications with IRCC).

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

Yes (see attached).

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**
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.	User is invited to visit BorderPass portal via a unique referral link from VIU in their offer letter.	N/A	
2.	All users acknowledge that the information collected is used for the purpose of filing immigration applications and consent to it being shared with IRCC.	N/A	
3.	Users sign-up/create profile with their email, first name, last name and student ID and then	Collection (BP)	s.26(c)
4.	Pres-Screening Assessment: applicant uploads required documents for the immigration process including passport, financial documents, and language test results Identity information such as gender, date of birth, phone number, and postal address, is also collected. Additionally, school, program, age, family information, visa history, criminal/medical information, financial information, and location may also be collected.	Collection and Use (BP)	s.26(c) and s. 32(a)
5.	BorderPass shares results from pre-screening with VIU.	Use & Disclosure to VIU; Collection by VIU	BP: s. 32(a) and s.33(2)(h); VIU: s.26(c) and s.27(1)(a)

6.	Users return to BorderPass to complete study permit application and track immigration status. Users provides necessary information (including passport information, VIU offer letter and other financial information) necessary to complete study permit application.	Collection and Use (BP)	s. 26(c) & 32(a)
7.	Users submit applications to BorderPass lawyers for review. Upload documents ranging from their passports, letters of acceptances and financial documentation as required for the purpose of submissions to IRCC.	Collection (BP lawyers)	
8.	Users submit applications to BorderPass lawyers for review	Collection	s.26(c)
9.	BorderPass Lawyers submit applications to IRCC	Disclosure	s.33(2)(d)
	Data Destruction policy outlined in data policy package	Retention	
	In summary, Students answer a series of assessment questions that are required by the BorderPass Legal team and IRCC for the purpose of services provided. BorderPass lawyers are subject to their own code of conduct and legal regulations under their respective provincial law societies and are held to the highest standards as it pertains to information collection. The information collected is proportionate to the goal of submitting high quality applications, ensuring compliance and increased approval success. BorderPass implements strict data security measures and only shares information with authorized/user consented parties. See attached Data Management Policy for more.		

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	Data breach of BP systems	SEE SOC II Report - These exact details are listed under the Report on Controls Relevant to Security, including but not limited to: • System features and configuration settings designed to authorize user access while restricting unauthorized users from accessing information not needed for their role; • Use of intrusion detection systems to prevent and identify potential security attacks from users outside the boundaries of the system; • Regular vulnerability scans over the system and network, and penetration tests over the production environment; and, • Operational procedures for managing security incidents and breaches, including notification procedures. • Use of encryption technologies to protect		

		customer data both at rest and in transit • Use of data retention and data disposal • Uptime availability of production systems		
2	User registers for account and creates weak password that they also use on unsecured sites. BP account is subsequently accessed by unauthorized user.	BP Password Policy and password encryption		
3	User personal information compromised in transit or on BP servers: User uploads sensitive documents (passport, financial docs, test results) and provides other sensitive info (criminal and health records, family info, gender, DOB, age, etc.)	• Data encrypted in transit and at rest in accordance with NIST standards. • Client's data protection complies with SOC 2 standards to encrypt data in transit and at rest, ensuring customer and company data and sensitive information is protected at all times.		
4	Unauthorized BP employee or contractor accesses student's PI	• BP implements role-based access controls and the principles of least privileged access, and review revoke access as needed.		

		• All BorderPass contractors and employees undergo background checks prior to being engaged or employed by BP in accordance with local laws and industry best practices. • Confidentiality or other types of Non-Disclosure Agreements (NDAs) are signed by all employees, contractors, and others who have a need to access sensitive or internal information. • BP embeds culture of security into their business by conducting employee security training & testing using current and emerging techniques and attack vectors.		
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.

https://www.borderpass.ai/privacy-policy

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?

AWS - 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 - as needed for immigration purposes as disclosed above

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 - as needed for immigration purposes as disclosed above

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)?**
Amazon	AWS	Amazon Servers 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.

See https://www.borderpass.ai/security and https://www.borderpass.ai/privacy-policy and Data Management Policy

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.

Not provided

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.

https://www.borderpass.ai/security + See Physical Security Policy in Data Management Policy attached
• Security perimeter with access control mechanisms; • Physical entry controls: access logs reviewed as necessary; cameras and intrusion detection systems used in areas with sensitive information • Restricted access to secure areas

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.

Please refer to : https://www.borderpass.ai/security, SOC II Report and Data Management Policy

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.

- BP determines access based on principle of least privilege.
- Utilizes Role-Based Access Control (RBAC)
- Wherever feasible, rights and restrictions shall be allocated to groups. Individual user accounts
- additional permissions granted as needed with approval from the system owner or authorized party.
- All privileged access to production infrastructure use Multi-Factor Authentication (MFA).

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.

- BP uses logging and monitoring of all type of system access.
- BP has implemented and maintained appropriate and reasonable organizational and technical security measures in line with recognized standard cyber security frameworks to protect against unauthorized or accidental access, loss, modification, disclosure, or destruction of Customer Data. See SOC II Report

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.

RBAC and system logs

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.

BorderPass ensures robust security and privacy through SOC II compliance, successful penetration testing, and AWS-secured data storage.

See SOCI II Report re: protection of sensitive information

See Data Management Policy Package.

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?**

VIU will not be involved in updates to information as this will be between the user and BorderPass. Users consent to an acknowledgment with respect to information shared with BorderPass. BorderPass Lawyers have the ability to correct personal information at the request of a user, and users are able to edit personal details accordingly prior to submission to IRCC. All details are logged in user communications and profile records.

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

No - BorderPass does not make decisions for users as this is the responsibility of IRCC.

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).

BP will retain your information as long as it's necessary to serve you or comply with legal obligations, and may hold it for up to ten years. You may request that we delete your information at any time. See Privacy policy Section 8: Retention of Personal Information for more details.

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
As disclosed above re: Personal Information
Name of main organization involved
AWS
Any other ministries, agencies, public bodies or organizations involved

Business contact title and phone number for person responsible for managing the Personal Information Bank
Sally Daub - CEO/Co-Founder - sally@borderpass.ai

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?

See Privacy Policy Section 2.5: Internal and External research, analysis, and partnership.

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.

Role	Name	Electronic signature	Date
Initiative lead	Director, Future Students		2025-03-03
Program/Department Manager (if different from initiative lead)			