Privacy Impact Assessment for:

Mobile Up – Alumni App

Initiative:	Mobile Up – Alumni App
Department or Service Area Name:	External Relations - Advancement and Alumni Relations

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.

Mobile Up (Alumni App) is a cloud-based digital communication platform used by the Office of Advancement and Alumni. The software supports the Alumni and Advancement Department in executing its fundraising initiatives, community and alumni engagement.

It is designed to seamlessly convert existing VIU webpages into a mobile friendly format. It allows VIU alumni to meaningfully engage in a digital format with their alumni and utilize existing digital infrastructure in a mobile friendly platform.

Mobile Up enables a secure platform to access their alumni card, share their businesses, access information about events, and the alumni benefits exclusive to them. It is an essential tool for alumni engagement. It also facilitates communication between the Advancement Department and our

alumni, informing them of benefits available to them as former VIU students and keeping them updated on programs related to their fields of study and alumni engagement events.

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?

Click or tap here to enter text. This PIA covers sign up and usage of the app. It covers what information is collected, by which party and for what purpose, how/where personal information is stored, and how personal information is used.

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.

N/A

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	First Name Last Name Email Communication Preferences Employment Information DOB VIU Credential Student Number
Contact details	Email Social Media
Account information	**Alumni:**

	Year of graduation and credential awarded
Commercial information	

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

Personal information is any recorded information about an identifiable individual, other than business contact information. Personal information includes information that can be used to identify an individual through association or reference.

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

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

Click or tap here to enter text.

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

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

Click or tap here to enter text.

Part 2 – Collection, Use, and Disclosure

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

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

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

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

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

Personal Information element	Does it meet all four points of the necessity threshold?	Reasons for keeping or excluding from initiative
First Name	Yes	Necessary to verify Alumni to sign into secure platform
Last Name	Yes	Necessary to verify Alumni to sign into secure platform
Email	Yes	Required to communicate with Alumni.
Communication Preferences	Yes	Necessary to communicate with alumni through their preferred channels, sharing only information that aligns with their interests.
Date of Birth: sometimes alumni forget their student numbers, so DOB is an alternate way to verify identities.	Yes	Necessary to identify Alumni to receive their alumni benefits.

VIU Education Credentials	Yes	Necessary for Alumni engagement
Student Number	Yes	Necessary to identify Alumni to receive their alumni benefits.

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

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

	Describe the way personal information moves through your initiative step by step as if you were explaining it to someone who does not know about your initiative.	**(Collection, Use or Disclosure)**	**FIPPA or other legal authority**
E.g.	*E.g., Student email, password, and IP address collected by software platform for account creation.*	*Collection*	*FIPPA 26(c) "info relates to and is necessary for a program or activity"*
	Alumni Information Flow		
1.	Alumni are imported from Raiser's Edge into the Mobile Up platform. **Reason:** Alumni encouraged to register on the Mobile Up App to access discounts, memberships, or services. The imported data is used during the verification process at registration.	Use (Communicate with Alumni and offer benefits) Disclosure (to MobileUp)	s. 32(a) s. 33(2)(d)
2.	Users (alumni) will input name and date of birth to verify status to access MobileUp app.	Use	s. 32(a)
3.	Users (alumni) can optionally input employment, address, and contact information voluntarily into a VIU webpage formatted to fit within the app if they would like to update their information. They do not need to do this to access or use the app. This information will not be stored within Mobile Up, rather Raiser's Edge.	Collection, Retention	s. 26(c)

2.2 Risk Mitigation Table

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

Risk Mitigation Table				
	Risk	**Mitigation Strategy**	**Likelihood**	**Impact/harm**
1	Selected services and business functions are provided by third parties.	Blackbaud has a Third Party Vendor Risk Management Program that evaluates third party risks before and during the business relationship. The evaluation is designed to fulfill their Cybersecurity Program requirements. (Blackbaud Data Security Addendum p2 Data Security Addendum.pdf) Blackbaud does no sell or share any personal information with third parties outside of the Target Analytics program. Target Analytics only applies to US individuals. (Blackbaud North American Privacy Policy North American Privacy Policy - Blackbaud) Through the use of cookies and web beacons third parties may obtain information such as the IP address of the computer that downloaded a web page, the URL of the web page, the time the web page was viewed and the type of browser used. Cookie	Medium	Possibility of unauthorised access, alteration, disclosure or destruction of data.

		configuring is set by the user at time of use. No personal information is included. (Blackbaud North American Privacy Policy North American Privacy Policy - Blackbaud)		
2	Data Breach/Data Loss	Blackbaud partners with Microsoft and Azure, giving them access to industry threat intelligence and early previews regarding upcoming feature capabilities and security releases. (Blackbaud Cyber Security Overview p3 Blackbaud Cyber Security Overview.pdf) Blackbaud performs several security assessments that [redacted] Blackbaud maintains compliance with PCI DSS (Payment Card Industry Data Security Standard) (Blackbaud Data Security Addendum p3 Data Security Addendum.pdf) [redacted] s. 15(1)(l) [redacted]	Medium	Possibility of unauthorised access, alteration, disclosure or destruction of data. Database may be venerable and open to cyber threats and ransomware attacks.

3	Unauthorized access	VIU employee access is granted through role-based permissions ensuring that employees only have access to the data and features of the database that are necessary to perform their tasks. Reviews are conducted annually and when new staff join the department. Blackbaud supports multi-factor authentication [redacted] s. 15(1)(l) Blackbaud provides on-going security awareness training for all its' employees and participates in global communities and platforms on best practices in the industry. (Blackbaud Cyber Security Overview p4 Blackbaud Cyber Security Overview.pdf) Blackbaud maintains a formal process to grant, prevent and terminate access to customer data. Access is limited to users who require such access to perform their job responsibilities and is based on least privilege roles. [redacted]	[redacted]	[redacted]

		[redacted] (Blackbaud Data Security Addendum p5 Data Security Addendum.pdf) s. 15(1)(l)		
4	Inadequate Data Encryption	Blackbaud uses strong encryption mechanisms, [redacted] (Blackbaud Cyber Security Overview p4 Blackbaud Cyber Security Overview.pdf)	Low	Sensitive donor information, such as personal details, payment methods, and donation history could be accessed by unauthorized individuals. This could lead to identity theft or fraudulent activities.

2.3. Collection or Privacy Notice

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

A collection notice must contain the following elements:

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

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

https://gov.viu.ca/access-and-privacy-viu

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.

Microsoft Azure's SQL Server, with automatic geo-redundancy and security monitoring, or Amazon Web Services, which uses Amazon GuardDuty to provide continuous Security Monitoring & Threat Detection.

3.1.1. Where is the personal information stored?

Click or tap here to enter text.
Microsoft Azure's SQL Server, with automatic geo-redundancy and security monitoring, or Amazon Web Services, which uses Amazon GuardDuty to provide continuous Security Monitoring & Threat Detection.

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.

No

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?

No

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)?**

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.

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

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.

Microsoft Azure's SQL Server, with automatic geo-redundancy and security monitoring, or Amazon Web Services, which uses Amazon GuardDuty to provide continuous Security Monitoring & Threat Detection.

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.

Industry Standard encryption for data in transit (TLS and SSL);
Microsoft Azure or AWS technical, physical, and logical security safeguards for data at rest.

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.

Click or tap here to enter text.

The security roles define the level of access and permissions users have to different parts of the system. The following roles have been implemented with some users having additional access as they are the backups for certain roles.

Administrator:

- Full access to all data and settings.
- Manages users, permissions, and system configurations.

Reporting and Data Analyst:

- Access to reporting tools and data analysis features.
- Can create run, view, and export reports

Custom Roles:
Being a small department is it essential that we have back-up systems in place to reduce interruptions during busy times and to allow for sick days and vacation schedules. Additional roles as assigned to users when they perform the backup tasks for one of their colleagues.

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.

Click or tap here to enter text.

Users with administration roles have access to the following logs:

Audit history of changes in roles:

- Adding users
- Marking users as inactive
- Admin status changes
- Role updates

Data Changes:

- Records added, modified, or deleted.
- Details of the changes, including before-and-after values (in some cases).

Export/Download Logs:

- Logs of data exports or downloads, including file names and user activity.

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.

Click or tap here to enter text.

RBAC- only authorized roles in the department will have access
Back-end access will be limited to the Alumni team (3 members). Each user will have their own 2FA to gain access to back-end accounts

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.

From Mobile Up Privacy Policy: MobileUp is committed to protecting the security of your Information and takes reasonable precautions to protect it. However, data transmissions over the internet, whether wired or wireless, cannot be guaranteed to be 100% secure. As a result, MobileUp cannot

ensure with 100% certainty the security of Information you transmit to us, including Personal Data or user generated content. Accordingly, you acknowledge and agree that you do so at your own risk. In order to minimize the security risk to your Information, MobileUp uses industry-standard encryption to protect your data in transit. This is commonly referred to as transport layer security ("TLS") or secure socket layer ("SSL") technology.
Once we receive your data, we protect it on Microsoft Azure or Amazon Web Services servers using a combination of technical, physical, and logical security safeguards. The security of the data stored locally in any of our Software installed on your devices requires that you make use of the security features of your device. We recommend that you take the appropriate steps to secure all devices that you use in connection with our Website, Software, or Services.

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?**

Click or tap here to enter text.

Updates to personal information are restricted to name changes, contact details, and communication preferences. Changes to gifts or donations require verification from the payment processing provider. All modifications are recorded in Blackbaud's audit log, which includes the date of the change, the requester, the individual who executed the change, and the reason for the update. Copies of emails or other communications with the donor are scanned and documented for record-keeping. Personal information is not disclosed to any other parties unless it is part of the data flow defined in this document and the Raiser's Edge PIA for Alumni to access their benefits.

To update their information with the Vancouver Island University (VIU) Alumni, a person can:

Email the Foundation: A person can reach out to the foundation via the alumni@viu.ca email. This email is listed on our website, tax receipts and all email communications.
They can then provide details of the changes required. Changes are typically made to the name or address, email or phone updates.
Online Update Form: VIU has on online form on our website where Alumni can submit updates to their address and communication preferences.
https://alumni.viu.ca/get-connected

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

Click or tap here to enter text.
No

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

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

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).

Click or tap here to enter text.
The VIU Records Management Program which includes the Records Classification and Retention Schedule (RCRS) is in development as of Fall 2025.

From Mobile Up Privacy policy: "Deleting your information from Mobile Up"
MobileUp allows you to delete your user account directly from the app or user website. You can also request that we delete your account by sending an email to our support team. Once we have verified your identity, we will be happy to assist in deleting your account. Additionally, please note that you must delete our Software from your device(s) in order complete the deletion process.

Please keep in mind that our deletion of your account does not delete the information that was collected by your organization. You will need to contact your organization directly if you wish to have your information deleted from their records.

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:

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?

Click or tap here to enter text.
Anonymous geographic sign in data will help us decide:

1. New discounts
2. Where to host Alumni events

Part 9 – Summary and Proponent Responsibility

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

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, Alumni and Advancement
Date:	2025-05-08