



<b>Initiative:</b>	Blackbaud Raiser’s Edge Fundraising software
<b>Department or Service Area Name:</b>	Alumni & Advancement, External Relations

**Part 1 – General Information and Overview ..... 1**

**Part 2 – Collection, Use, and Disclosure ..... 5**

**Part 3: Storing Personal Information..... 19**

**Part 4: Assessment for Disclosures of Sensitive Personal Information ..... 19**

**Part 5: Security of Personal Information ..... 21**

**Part 6: Accuracy/Correction/Retention of Personal Information ..... 26**

**Part 7 – Personal Information Banks..... 28**

**Part 8 – Further Information..... 29**

**Part 9 – Summary and Proponent Responsibility ..... 29**

**Part 10: Signatures..... 30**

## 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.

Raiser's Edge NXT is a cloud-based fundraising platform used by the Office of Advancement and Alumni. The software supports the Alumni and Advancement Department in executing its fundraising initiatives, which focus on providing student support through scholarships, awards, and bursaries. Additionally, the department leads efforts to raise funds for program support across various university departments and occasionally undertakes capital campaigns.

Raiser's Edge NXT enables the secure processing of online donations and the issues of tax receipts to donors in accordance with Canada Revenue Agency (CRA) guidelines. It is an essential tool for donor management, fundraising reporting and stewardship initiatives. 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.

Raiser's Edge is a comprehensive tool for managing donor and alumni relationships and fundraising activities. It is used in the following activities:

### **Donor Management**

Raiser's Edge allows solicitors to carry out their fundraising activities by giving them access donor profiles, contact details, giving history, interests and engagement levels. In addition, Raiser's Edge stores gift agreements. Fundraisers use Raiser's Edge to track their prospect through the donor life cycle - identification, cultivation, solicitation, stewardship.

### **Fundraising Campaigns/Appeals**

The department uses Raiser's Edge to effectively set up, monitor, and manage a variety of fundraising campaigns and appeals, such as the annual Giving Tuesday initiative. The platform enables the team to streamline campaign planning, track donor engagement, and assess the overall success of each appeal.

### **Gift Processing:**

Raiser's Edge is used to record, process, receipt, and acknowledge a variety of donations, including online gifts, gifts-in-kind, shares, cash, cheques, payroll deductions, and electronic funds transfer (EFT) transactions. The system tracks outstanding pledges and supports recurring gifts, enabling the department to manage solicitation renewals to ensure student awards are fully funded at the correct time each year. Additionally, Raiser's Edge export tools facilitate the transfer of gift information to the finance department for accurate accounting entries.

### **Reporting and Analytics:**

Raiser's Edge performs on-demand data analysis that allows the department to analyze donor trends, renewals rates and campaign performance and other key metrics related to fundraising. Through Raiser's Edge, the department ensures a data-driven approach to fundraising, optimizing strategies to maximize donor participation and financial support.

### **Stewardship and Engagement:**

The stewardship department utilizes Raiser's Edge around various donor-related activities. This includes distributing student thank-you cards to donors, generating and distributing endowment reports, and producing student recipient reports. The platform supports the department in fostering

strong relationships with donors and is also used to create targeted lists for e-newsletters, alumni notifications, and stewardship event communications. It automates the generation of thank-you letters and tracks all email interactions with alumni and donors.

### 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 Address Email Phone number Family status Communication Preferences Relationships between donors  <b>For Organizations these additional elements are included:</b> Contact name, position, phone number, business address, business phone and business email.  <b>For Alumni these additional elements are included:</b> Date of Birth, VIU Education Credentials, Student Number,
Contact details	Address Email Phone number
Account information	<b>Alumni:</b> Year of graduation and credential awarded

	<p><b>From Donors:</b> Awards and funds associated with the donor's gift, gift agreements, dollar amount of donation, how the donation was paid (Cheque, EFT etc...) intention of the contribution.</p>
Commercial information	<p><b>Donation Amount</b> Method of payment (e.g. cash, cheque, credit card) The purpose of the gift (it's designation or intended use e.g. student support, programming, endowments)</p>

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	
<ul style="list-style-type: none"> <li>Name, age, sex, weight, height</li> <li>Home address, phone number</li> <li>Race, ethnic origin, sexual orientation</li> <li>Medical information</li> <li>Health history</li> <li>Number or symbol assigned to the individual</li> <li>Income, purchases and spending habits</li> <li>Blood type, DNA code, fingerprints</li> </ul>	<ul style="list-style-type: none"> <li>Marital or family status</li> <li>Religion</li> <li>Education</li> <li>Financial information</li> <li>Criminal information</li> <li>Employment information</li> <li>Personal views or opinions, except if they are about someone else</li> </ul>

- If yes, go to [Part 2](#)
- If no, answer question 1.5 and submit questions 1 to 1.5 to [privacy.officer@viu.ca](mailto: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 issue tax receipts and to communicate with donors using the correct salutation.
Last Name	Yes	Necessary to issue tax receipts and to communicate with donors using the correct salutation.
Address	Yes	Necessary to issue tax receipts and to

		<b>communicate with donors and prospects</b>
<b>Email</b>	<b>Yes</b>	<b>Required to communicate with donor.</b>
<b>Phone Number</b>	<b>Yes</b>	<b>Required to communicate with donor.</b>
<b>Marital or family status</b>	<b>Yes</b>	<b>Necessary to communicate with donors using the correct salutation.</b>
<b>Communication Preferences</b>	<b>Yes</b>	<b>Necessary to communicate with donors and alumni through their preferred channels, sharing only information that aligns with their interests.</b>
<b>Date of Birth: sometimes alumni forget their student numbers, so DOB is an alternate way to verify identities.</b>	<b>Yes</b>	<b>Necessary to identify Alumni to receive their alumni benefits.</b>
<b>VIU Education Credentials</b>	<b>Yes</b>	<b>Necessary for Alumni engagement</b>
<b>Student Number</b>	<b>Yes</b>	<b>Necessary to identify Alumni to receive their alumni benefits.</b>

## 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.

	<b>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.</b>	<b>(Collection, Use or Disclosure)</b>	<b>FIPPA or other legal authority</b>
<i>E.g.</i>	<i>E.g., Student email, password, and IP address collected by software platform for account creation.</i>	<i>Collection</i>	<i>FIPPA 26(c) "info relates to and is necessary for a program or activity"</i>
	<b>Donor Information Flow</b>		
1.	<p>Donor fills out donation form: First name, last name, address, email, phone. This information is captured in several different ways depending on the method of payment:</p> <ul style="list-style-type: none"> <li>• Cash and Cheque (emails donation form to VIU Foundation)</li> <li>• Online Donation (online form)</li> <li>• Payroll Deduction (internal online payroll deduction form)</li> <li>• Electronic File Transfer (emails donation form to VIU Foundation)</li> </ul> <p><b>Reason:</b> To issue tax receipt and communicate with donor.</p>	Use, Collection	FIPPA 26(c) CRA rules for issuing tax receipts
2.	<p>Cheques and payment forms are scanned, and these copies are saved on the Advancement and Alumni shared drive. Any gift agreements, award terms of reference or documentation showing gift intention are also included.</p> <p>Online donations forms are saved as .pdf documents as confirmation of the donation, the amount and the intention of the gift. The information will be retained for seven years as per CRA tax guidelines.</p>	Use, Collection, Retention	FIPPA 26(c); 32(a) CRA guidelines

	<p><b>Reason:</b> Copies are required for audit purposes and to confirm the intent of the gift.</p>		
3.	<p>Donor information is entered onto Raiser's Edge</p> <p><b>Reason: For accurate financial tracking, donor stewardship, compliance with CRA guidelines for charities, to generate CRA compliant tax receipts.</b></p>	Use, Disclosure	FIPPA s. 32(a); s. 33.2(a)
3a.	<p>Donor communication preferences are exported from Constant Contact and imported to Raiser's Edge. Constant Contact (email client): Constant Contact stores information on emails sent, clicks, opens, and unsubscribes. This information is downloaded to an excel file and imported to RE using Importacular desktop version. This will soon transition to an online version of Importacular. The information is connected using the donor's email address and the information is not stored in Importacular.</p> <p><b>Reason:</b> It is important to stay up to date on email solicit codes to ensure we are within CASL requirements. Analysis is performed on Donor Engagement (clicks and opens of emails) to determine if it fosters more donations or event participation.</p>	<p>Collection (donor email preferences; engagement analytics).</p> <p>Use (analyze email engagement metrics);</p> <p>Disclosure (to RE)</p>	<p>s. 26(c)</p> <p>s. 32(a)</p> <p>s. 33(2)(d)</p>
4.	<p>Donor name, gift amount and fund (intention of the gift) is added to Fledger/SAGE. (Fledger and Sage are accounting management systems that VIU Financial uses to disperse awards to students.</p> <p><b>Reason:</b> To maintain accurate financial records with VIU, to ensure that awards are disbursed to student or programs.</p>	Use, Disclosure	FIPPA s. 32(a); s. 33(2)(d)(p)(i)

5.	The President's Office is notified of gifts in kind, including name, amount and a description of the gift in kind  <b>Reason:</b> Transfer of in-kind gifts to VIU	Disclosure	s. 33(2)(d)
6.	Award terms of reference and relevant donor information is sent to Financial Aid through the Award Management System.  <b>Reason:</b> For Financial Aid to determine when students meet the criteria for the award to be disbursed.	Use, Disclosure	FIPPA s. 32(a); s. 33(2)(d)
7.	Award terms of reference are posted on VIU web site. May include the donor's or organization's name  <b>Reason:</b> For students to have the opportunity to apply for the award	Use, Disclosure	FIPPA s. 32(a); s. 33(2)(d)
8.	Donor names and contact details are sent the departments that have been supported.  <b>Reason:</b> To give deans and program heads the opportunity to directly thank donors for supporting their project as part of the on-going stewardship plan.	Use, Disclosure	FIPPA s. 32(a); s. 33(2)(d)
9.	Donor notifies department via email if any changes need to be made to their salutation and other communication preferences  <b>Reason:</b> To correctly address the donor through communications	Collection	FIPPA s. 26(c)

	<b>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.</b>	<b>(Collection, Use or Disclosure)</b>	<b>FIPPA or other legal authority</b>
E.g.	<i>E.g., Student email, password, and IP address collected by software platform for account creation.</i>	<i>Collection</i>	<i>FIPPA 26(c) "info relates to and is necessary for a program or activity"</i>



<b>Alumni Information Flow</b>			
1.	<p>Alumni information (<b>Date of Birth, VIU Education Credentials, Student Number,</b>) from the Student Record System is prepared for import and placed in a folder shared by authorized individuals from Student Records and the Advancement and Alumni Department. The data coordinator imports this data into Raiser's Edge NXT</p> <p><b>Reason:</b> For the department to maintain an accurate record of Alumni and their contact details.</p>	Collection	FIPPA s. 26(c)
2.	<p>Alumni information from the Student Record System is prepared for import and placed in a private folder shared by authorized individuals from Student Records and the Advancement and Alumni Department. This information is downloaded to an excel file and imported to RE using Importacular desktop version. This will soon transition to an online version of Importacular. The information is connected using the alumni/student number and the information is not stored within the import client.</p> <p><b>Reason:</b> Congratulations sent to graduates via email with a welcome to the VIU Alumni community. Alumni are notified via email of the services and discounts that are available to them.</p>	Use, Disclosure	s. 23(2); s. 33(2)(d)(h)
3.	<p>Alumni receive e-newsletters, invitations to events, and updates from various faculties and departments. They are also included in fundraising initiatives, such as Giving Tuesday, and are offered opportunities to participate in surveys or volunteer as mentors for current VIU students. Emails are sent using Constant Contact.</p>	Use	s. 32(a)

	<p><b>Reason:</b> To keep alumni connected, foster pride and belonging, solicit donations for scholarships and initiatives, and share updates on university projects and programs.</p>		
3a.	<p>Constant Contact (email client): Constant Contact stores information on emails sent, clicks, opens, and unsubscribes. This information is downloaded to an excel file and imported to RE using Importacular desktop version. This will soon transition to an online version of Importacular. The department may also pilot EasyREImport for this purpose. The information is connected using the alumni/student number and the information is not stored within the import client.</p> <p>It is important to stay up to date on email solicit codes to ensure we are within CASL requirements.</p> <p>Analysis is performed on Alumni email engagement (clicks and opens of emails) to determine if it fosters more donations or event participation.</p>	<p>Use</p> <p>Disclosure</p>	<p>s. 32(a)</p> <p>s. 33(2)(d)</p> <p>CASL requirements</p>
4.	<p>Alumni are imported from Raiser's Edge into the MobileUp App.</p> <p>An excel list from Raiser's Edge is downloaded including alumni:</p> <ul style="list-style-type: none"> <li>• Name</li> <li>• Student Number</li> <li>• Birth Date (to confirm identity)</li> <li>• Email</li> <li>• Address</li> <li>• Grad Year</li> <li>• Degree</li> </ul>	<p>Use, Disclosure</p>	<p>s. 32(a)</p> <p>s. 33(2)(d)</p>

	<p>This list is uploaded to MobileUp using an admin account and password.</p> <p><b>Reason:</b> Alumni are encouraged to register on the MobileUp App so they can access discounts, memberships, or services. The imported data is used during the verification process at registration.</p>		
5.	<p><b>AFFILIATION PARTNER, TD INSURANCE</b></p> <p><b>Eligibility List Upload</b>          Alumni lists are securely transferred to our affiliation partner, TD Insurance, to allow the inquiring members to have access to preferred rates. VIU uploads all eligible alumni (who haven't opted out) including their:</p> <ul style="list-style-type: none"> <li>• Name</li> <li>• Address</li> <li>• Email</li> </ul> <p>TD Insurance requires VIU to upload this list to the secure software Tibco. The request is sent by the relationship manager who provides a password. The link to the portal is <a href="https://mfttisp.td.com:10443/cfcc/login/login.jsp">https://mfttisp.td.com:10443/cfcc/login/login.jsp</a>.</p> <p>Alumni can unsubscribe from the TD emails or any VIU Alumni email to opt-out of further email campaigns. They can also email <a href="mailto:alumni@viu.ca">alumni@viu.ca</a> to unsubscribe from future correspondence.</p> <p><b>Cossette sFTP (secure File Transfer Protocol) for TD Insurance Affinity emails: Unsubscribe file retrieval</b></p> <p>An sFTP , WinSCP, is required to access the sFTP server where the unsubscribe files from the above alumni campaign are securely downloaded.</p>	Use, Disclosure	

	<p>sFTP requires two different applications to function. The Server (host - Cossette) and Client (accessor) applications. The Server application is installed on server computer, which allows the server to become a gateway to host and exchange information.</p> <p>This information is downloaded to an excel file and imported using Importacular desktop version. The information is connected using the alumni's email address and the information is not stored in Importacular.</p> <p>Reason: Alumni are provided with opportunities to access exclusive discounts on life insurance, home insurance, critical illness insurance, and various other services offered through our affiliate partners.</p>		
--	--	--	--

## 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	Medium	Possibility of unauthorised access, alteration, disclosure or destruction of data.

Blackbaud Raiser's Edge Fundraising software

		<p>requirements. (Blackbaud Data Security Addendum p2 <a href="#">Data Security Addendum.pdf</a> )</p> <p>Blackbaud does not 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 <a href="#">North American Privacy Policy - Blackbaud</a>)</p> <p>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 configuring is set by the user at time of use. No personal information is included. (Blackbaud North American Privacy Policy <a href="#">North American Privacy Policy - Blackbaud</a>)</p>		
2	Data Breach/Data Loss	<p>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 <a href="#">Blackbaud Cyber Security Overview.pdf</a>)</p>	Medium	<p>Possibility of unauthorised access, alteration, disclosure or destruction of data.</p> <p>Database may be vulnerable and open to cyber threats and ransomware attacks.</p>



Privacy Impact Assessment for:

Blackbaud Raiser's Edge Fundraising software

		<p>Blackbaud performs several security assessments that include penetration testing, software security testing and audits. Blackbaud maintains compliance with PCI DSS (Payment Card Industry Data Security Standard) (Blackbaud Data Security Addendum p3 <a href="#">Data Security Addendum.pdf</a> )</p> <p>Blackbaud has a comprehensive incident response process that focuses on identification, notification, containment, eradication and recovery (Blackbaud Incident Management and Response Overview <a href="#">Blackbaud Incident Management and Response Overview.pdf</a>)</p>		
3	Unauthorized access	<p>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.</p> <p>Blackbaud supports multi-factor authentication and uses identity providers (IdP) such as Microsoft Azure Active Directory, Okta, Google G-Suite to provide</p>	Medium	Employees could access personal information and use or disclose it for personal purposes.

Blackbaud Raiser's Edge Fundraising software

		<p>authentication. (Blackbaud Cyber Security Overview p4 <a href="#">Blackbaud Cyber Security Overview.pdf</a>)</p> <p>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 <a href="#">Blackbaud Cyber Security Overview.pdf</a>)</p> <p>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. For password access Blackbaud enforces multifactor authentication, complex passwords and password expiration procedures. (Blackbaud Data Security Addendum p5 <a href="#">Data Security Addendum.pdf</a> )</p>		
4	Inadequate Data Encryption	<p>Blackbaud uses strong encryption mechanisms, including TLS 1.2, AES 256, RSA 1024 and other FIPS140-2 encryption algorithms. (Blackbaud Cyber Security Overview p4 <a href="#">Blackbaud Cyber Security Overview.pdf</a>)</p>	Low	Sensitive donor information, such as personal details, payment methods, and donation history could be accessed by unauthorized



Privacy Impact Assessment for:

Blackbaud Raiser's Edge Fundraising software

				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.

#### Privacy Statement on <https://alumni.viu.ca/get-connected>

The personal information you provide on this form is collected pursuant to section 26 of the British Columbia Freedom of Information and Protection of Privacy Act. This information is collected for the intended purposes of the form. Your personal information will be accessible only by authorized Vancouver Island University employees (VIU) and representatives, or as otherwise permitted by law. This information will be kept on secure servers, including a server located outside of Canada. Questions about the collection of your personal information should be directed to [alumni@viu.ca](mailto:alumni@viu.ca).

**Vancouver Island University and Vancouver Island University (VIU) Alumni is committed to protecting the privacy and the personal information of its alumni and other stakeholders. We value the trust of those we deal with, and of the public.** Any information that you choose to provide will be protected in accordance with applicable [privacy legislation](#) and Vancouver Island University's [policies and procedures](#). The information on this form is collected under the legal authority of the [University Act](#).



Privacy Impact Assessment for:

Blackbaud Raiser's Edge Fundraising software

Vancouver Island University and VIU Alumni will only use your personal information for the stated purposes for which it was collected, unless you provide consent otherwise. Your personal information will only be disclosed to or accessed by Vancouver Island University employees and VIU Alumni with a need to know in relation to the purposes for which it was collected. Vancouver Island University and VIU Alumni will not sell or rent your personal information to any third parties. The information provided will **only be used for alumni-related activities and communications** between you, Vancouver Island University, and VIU Alumni.

If you have questions about the collection and use of this information, or would like to limit the kinds of contact you receive, please contact [Alumni@viu.ca](mailto:Alumni@viu.ca).

<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.

No - Data Center will be in Toronto, ON. Blackbaud [REDACTED] **s. 15(1)(l)**  
[REDACTED] The data centres are physically secure, have fire detection and suppression, heating, ventilation and air conditioning. (Data Centers for Hosted Customers [Data Centers for Hosted Customers.pdf](#))

#### 3.1.1. Where is the personal information stored?

Click or tap here to enter text.  
Toronto, ON [Data Centers for Hosted Customers.pdf](#)

### 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 – Credit Card Information for online transactions, giving history of a donors

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)?
Blackbaud Merchant Services  <a href="#">Secure Payment Processing &amp; Merchant Services for Nonprofits   Blackbaud</a>	Blackbaud SKY UX via AWS	Data stored in the United States in Amazon Web Services. BBMS has the ability to de-identify data in Merchant Services Portal.
Blackbaud	Microsoft Azure	Data centre is in Toronto, backups in Quebec City

**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.

Click or tap here to enter text.

Blackbaud is compliant with the **Payment Card Industry Data Security Standards (PCI DSS)**, which provides guidelines for securely processing, storing, and transmitting credit card data. Credit card information is not stored in Blackbaud systems. Sensitive data is replaced with tokens, which cannot be used if intercepted. Credit card data is encrypted during transmission and storage and cannot be read without decryption keys. Credit card information is only used to process the donation online and at no time is the full credit card number or cvv available to VIU employees.

<https://www.blackbaud.com/security/pci-compliance>

**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.

Click or tap here to enter text.

Contact is under negotiation. To be signed by Dec 1, 2024.



The contact describes the responsibilities of both parties regarding their obligations regarding privacy and security. Blackbaud commits to providing security summaries when breaches occurs and to provide notification of security breaches within 72 hours of Blackbaud becoming aware of the security breach. Blackbaud will provide information regarding the nature and consequences of the breach. Blackbaud will take reasonable measures to mitigate the cause of the security breach and will engage in reasonable corrective measures to prevent further breaches.

## 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.

[REDACTED]

s. 15(1)(l)

[REDACTED] and exterior of the facilities 24 hours a day, 365 days a year.  
(Data Centers for Hosted Customers p1)

Blackbaud's datacenters provide industry standard power management, heating/ventilation/air conditioning, fire detection and suppression, continuous monitoring, and access to intelligent IP networks. (See Blackbaud Data Security Addendum p3)

Blackbaud requires that employees, agents and subcontractors are subject to an appropriate duty of confidentiality (See Blackbaud Data Security Addendum p3)

Blackbaud provides its personnel with information security training upon hire and at least annually thereafter. (See Blackbaud Data Security Addendum p3)

[Data Centers for Hosted Customers.pdf](#)  
[Blackbaud Cyber Security Overview.pdf](#)

**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.

**Encryption**

Blackbaud uses various strong encryption mechanisms across their environments and products, including [REDACTED] encryption algorithms. (Blackbaud Cyber Security Overview p4 [Blackbaud Cyber Security Overview.pdf](#))

s. 15(1)(l)

**Multifactor authentication**

Through Blackbaud ID, they support multi-factor authentication and modern identity providers (IdP) such as [REDACTED] (Blackbaud Cyber Security Overview p4 [Blackbaud Cyber Security Overview.pdf](#))

**Passwords**

For password access Blackbaud enforces multifactor authentication, complex passwords and password expiration procedures:

Passwords must be complex and meet relevant industry frameworks, including the following:

- minimum length.
- characters of different types: alpha, numeric, and special characters.
- not be the same as the User ID with which they are associated.

Blackbaud enforces password expiration at regular intervals in accordance with relevant industry frameworks.

When providing users with a new or reset password, or other authentication credentials, Blackbaud uses a secure method to provide this information and maintain a written policy requiring reset at first login whenever a temporary credential is used.

(Blackbaud Data Security Addendum p5 [Data Security Addendum.pdf](#) )

**Firewalls**

Blackbaud maintains security measures for its network and supporting infrastructure, including, network security protocols, network identification services, firewall protection, intrusion detection and intrusion prevention systems, and periodic vulnerability scans for the relevant Solutions.

(Blackbaud Data Security Addendum p1 [Data Security Addendum.pdf](#) )

Blackbaud uses the Security Information and Event Management (“SIEM”) toolset to proactively monitor for security, event, and performance-related issues. Blackbaud’s firewall systems in provides visibility into network activities, violations and anomalies are reported as alerts for prompt action. (Blackbaud Data Security Addendum p4 [Data Security Addendum.pdf](#) )

### **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.
- Managers users, permissions, and system configurations.

#### **Fundraisers and Stewardship:**

- Access to donor information, gifts, and interactions.
- Can track and manage fundraising activities and actions
- Cannot add gifts or issue receipts
- Cannot modify reports

#### **Gift Processor:**

- Access to record and process donations and issuing receipts

#### **Reporting and Data Analyst:**

- Access to reporting tools and data analysis features.

- Can create run, view, and export reports

**View-Only User:**

- Can view data but cannot make changes or enter new information.

**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.

**Blackbaud has an Incident Response Management Plan in place for unauthorized access. Blackbaud will provide notification of breach within 72 hours of becoming aware of a use, access, or disclosure of client confidential information in Blackbaud's possession that is not**

permitted by the terms of our agreement. Notification will be via email, and they will provide a written report describing the circumstances surrounding the incident. Blackbaud would immediately initiate an investigation and will work with us to determine notification requirements. [Blackbaud Incident Management and Response Overview.pdf](#)

### 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.

Raiser's Edge NXT has permissions for record types that are managed based on user roles.

#### **View Permissions:**

Users with view permissions can access and read records of specific types (e.g., constituents, gifts, accounts). This ensures they can review details without altering data.

#### **Add Permissions:**

Users with add permissions can create new records in the allowed categories, such as adding a new constituent or transaction.

#### **Delete Permissions:**

Users with delete permissions can remove records from the system. Deletion permissions restricted to administrator roles due to the importance of maintaining data integrity and audit trails.

### 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.

Click or tap here to enter text.

Blackbaud implements several technical measures and controls to prevent unauthorized access to personal information. These include:

### **Data Encryption**

Data is encrypted both in transit (using SSL/TLS protocols) and at rest to protect sensitive information.

### **Access Control**

Role-based access ensures users only have access to the data and tools necessary for their job functions.

Multi-factor authentication (MFA) is used to enhance account security.

### **Network Security**

Firewalls and intrusion detection/prevention systems (IDS/IPS) monitor and block unauthorized access attempts.

Regular vulnerability assessments and penetration testing are conducted.

### **Incident Response Plan**

There is an incident response plan in place that ensures a swift reaction to any breach attempts or incidents.

[Data Security Addendum.pdf](#)

## **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 flow of the process flow defined in this document for Alumni to access their benefits.

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

**Email the Foundation:** A person can reach out to the foundation via the [foundation@viu.ca](mailto:foundation@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.

**Phone the Foundation:** A person can directly call the VIU Foundation's office to update their records. This phone number is listed on our website and in all email communications.

**Online Update Form:** VIU has an online form on our website where Alumni can submit updates to their address and communication preferences.  
<https://alumni.viu.ca/get-connected>

**Mail or In-Person Visit:** There are also options for donors to mail in changes or personally visit the Foundation office.

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

Click or tap here to enter text.

Personal information may be used for donor recognition purposes. Donors may be recognized through publications, event and through social media. Donor recognition requires a signed gift agreement between the two parties. Through their gift agreements donor's have the option to have an award, or an endowment named after them.

The Foundation may analyze donor histories and interests to tailor fundraising campaigns or solicitations.

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).

Click or tap here to enter text.

The VIU Records Management Program which includes the Records Classification and Retention Schedule (RCRS) is under development.

## 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?

Click or tap here to enter text.

Yes – The donor giving history is stored on the database

If yes, please complete the table below:

Describe the type of information in the bank
--

Giving history, gift agreements, signed terms of reference, endowment contacts
--

<b>Name of main organization involved</b>
Vancouver Island University Foundation
<b>Any other ministries, agencies, public bodies or organizations involved</b>
N/A
<b>Business contact title and phone number for person responsible for managing the Personal Information Bank</b>
██████████, Manager Advancement Services, ██████████

s. 22(1)

## 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?**

<p>Click or tap here to enter text.</p> <p>The Foundation may analyze donor histories and interests to tailor fundraising campaigns or solicitations.</p> <p>Responses from alumni surveys will be used for statistical purposes. Personal information is not used for statical purposes. In some cases, the postal code or the city is used to segment data.</p>
---

## Part 9 – Summary and Proponent Responsibility

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

<ul style="list-style-type: none"> <li> <div style="background-color: black; color: white; padding: 5px; display: inline-block;">s. 13(1)</div> </li> </ul>
---





Privacy Impact Assessment for:

## Blackbaud Raiser's Edge Fundraising software

*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.*

<b>Reviewed by</b>	Privacy Officer
<b>Approved by</b>	Manager, Advancement Services
<b>Date:</b>	26-Nov-2024