Part 1 – General

Name of Department/Branch	University Advancement + Events		
PIA Drafter:	Audrey Chen		
Email:	audreychen@ecuad.ca	**Phone:**	605-844-3886
Program Manager:	Chantale Lavoie		
Email:	clavoie@ecuad.ca	**Phone:**	604-844-3078

1. Description of the Initiative

This description and the following sections limit the scope of the PIA to the impact that the changeover to NXT will have.

This project will upgrade the Raiser's Edge system to a SaaS version called Raiser's Edge NXT. The Raiser's Edge system will migrate from ECU to Blackbaud hosting services.
The following Raiser's Edge system components will be changed as a result of this project:
1. Raiser's Edge CRM interface (current state)
   - Desktop application installed on client workstations.
   - Remote application launched from client workstations.
   - Clients (the users) use their Raiser's Edge account and password to sign in (not single sign-on).

2. Raiser's Edge database server (current state)
   - All CRM data is stored on the database server.
   - The CRM application connects to the database server.
   - Hosted at ECU.

The following Raiser's Edge system component changes will occur as a result of this project:
1. Raiser's Edge CRM interface (changed state)
   - Individual user accounts are provisioned, with various levels of read/write access.
   - Users access the interface from desktop and mobile devices using a standard web browser.
   - Users' security levels are customized (read/write access will be customized to each user)

- Two web browser versions are available:
    i. NXT web view, which is a mobile-optimized instance of the RENXT service.
    ii. Database view enabled with a Citrix web browser add-on, which is the main, desktop-based instance of the service.
- Blackbaud hosts the CRM application.
- Previous desktop applications will be un-installed from client workstations.

2. Raiser's Edge remote application server (changed state)
    - This server is no longer required at ECU and will be decommissioned once the migration and transition to RENXT is confirmed to be functioning appropriately. Suggested timeline for decommissioning the on-site server is 1 year.

3. Raiser's Edge database server (changed state)
    - All CRM data stored on the database server will be migrated to the new Blackbaud hosting environment, stored in Microsoft Azure servers in Ontario, Canada.
    - This server is no longer required at ECU and will be decommissioned.

4. Users will be able to access Raiser's Edge Analytics module: this includes access to a variety of pre-built reports, as well as custom generated reports and visual analytics. For fundraising, the metrics include relevant statistics such as page views, conversion rate, and average donation. For email marketing, the metrics include relevant statistics such as open rates, click through rates, and average gift amount.

The implications of the changes that will be the result of the project in terms of FIPPA are as follows.

FIPPA section 30.1 storage and access must be in Canada:
- All CRM data and personal information stored in the Raiser's Edge database server will be migrated from ECU to data centres hosted by Blackbaud and located in Canada: no implications for FIPPA so long as those Blackbaud's information infrastructure remains in Canada.
- Blackbaud must ensure that personal information in its custody is stored only in Canada and accessed only in Canada: again, no implications so long as the Blackbaud information infrastructure remains in Canada.
- Backup and failover data must also be stored in Canada: again, no implications so long as the Blackbaud information infrastructure remains in Canada.
- Blackbaud staff located in Canada will have administrative access to personal information stored in the systems: FIPPA permits the university's service providers to have restricted access on a need-to-know basis to personal information that the university has collected but that access must be secured against unauthorized collection, use, access, disposal, disclosure,

or other interference; accordingly, contractual obligations will be used to ensure that Blackbaud and the university do not make use of unauthorized access to personal information.

- Controls must be in place to ensure that Blackbaud staff located outside of Canada do not have administrative access to personal information stored in these systems: FIPPA does not permit access to personal information from outside of Canada except in accordance with ss. 30.1(by consent or for other permissible purposes), 33.1(1)(e) (for access temporarily from outside Canada), and 33.1(1)(i.1) (for processing payments); accordingly, contractual obligations will be used to ensure that Blackbaud and the university meet their obligations to restrict access to personal information from outside Canada.

The university will at all times retain control of personal information in RENXT, even where Blackbaud has functional custody over that information. Blackbaud will be retained as a service provider and part of the contractual agreement between the parties will stipulate that the university will retain control of personal information at all times, even if some of that personal information comes into the custody of the university's service providers as they perform authorized functions for the university. Blackbaud may aggregate information from the use of RENXT with information from other customers' use, and use and disclose such results on an aggregated and anonymized basis. Data ownership is outlined in Section 11 of the Blackbaud Solutions Agreement:
https://www.blackbaud.com/files/blackbaudsolutionsagreement.pdf

As a result of this project, an exact copy of the current Raiser's Edge database will be made to migrate to the new system. The Raiser's Edge database and the records stored in the database do not change.

The NXT system including the Raiser's Edge database is hosted on the Microsoft Azure platform, which is located in Toronto, Ontario, Canada.
The migration of the Raiser's Edge database to the new system follows these steps:
1. ECU Systems creates a backup file from the current Raiser's Edge production database located at ECU.
2. ECU Systems transfers the database backup file via secure ftp to the secure file server at the new Blackbaud hosting environment.
3. Blackbaud restores the backup file to the new Raiser's Edge database server.

Blackbaud Merchant Services would be an option for processing credit card payments. If implemented, donors would enter and submit their payment information on the ECU website, and their payment will be processed using BBMS. BBMS servers are located in the United States. Blackbaud encrypts personal and credit card information during all transactions, and sends an automated confirmation email for all payments. BBMS is compliant with the Payment Card Industry (PCI) Data Security Standard; it adheres to the PCI-DSS through encrypting and tokenizing all card information, and having implemented fraud mitigation tools. The BBMS Privacy Shield Certification Notice can be found here:
https://www.blackbaud.com/company/privacy-shield-notice

2. Scope of this PIA

This section limits the scope of the PIA to the impact that the changeover to NXT will have.

The Raiser's Edge system is used to perform the same tasks on both the current system and the upgraded system. This PIA does not cover the day-to-day use of Raiser's Edge NXT.
The significant change is not how the clients use the system but rather how they access the system.
RENXT will be used for the purposes of managing the following:

- Alumni engagement (events, volunteers, academic history, communications);
- Prospective donors (research, ratings, assignment to fundraisers);
- Fundraising activities (identification, cultivation, solicitation, stewardship);
- Gift processing (accepting payment, issuing receipts, posting to general ledger);
- Event registration processing (accepting payment, importing participants);
- Constituent information updates (biographical, contact, relationships, attributes);
- Reports (dashboards, query building, export to excel file);
- Analytics (via Raiser's Edge Analytics module called "SKY Reporting")
- Imports (add or update records from an excel file); and
- System administration (user account provisioning, application configuration, database backup).

How RENXT is to be used:

- Clients access the 'NXT web view' using a web browser on a desktop or mobile device;
- Clients access the 'Citrix database view' using a web browser on a desktop; and
- System administrators access a backup file of the Raiser's Edge database from a secure FTP server hosted by Blackbaud.

Who uses RENXT:

- University Advancement + Events employees (approximately 7 staff), and perhaps IT for support

FIPPA section 30.1 storage and access must be in Canada:

- The backup file of the Raiser's Edge database is stored on a secure FTP server that is located in Canada and it is intended only to be accessed by ECU clients from within Canada.

The scope of this PIA also includes BBMS (Blackbaud Merchant Services), which is a merchant account responsible for processing credit card transactions. Currently, the university uses CanadaHelps, a Canadian solution. BBMS uses servers located in the United States.

3. Related Privacy Impact Assessments

N/A

4. **Elements of Information or Data**

   Data categories on the existing RE database include donor information:

   1. Bio 1
      - Includes name, title, ID, gender, birthdate, spouse, address, phone, email website, education (grad year, major, etc.), business, bank (which we don't use)
   2. Bio2
      - Includes Constituent Codes and associated dates
   3. Addresses
      - Current and past addresses
   4. Addressees/Salutation
   5. Relationships
      - Includes connections to people (i.e. family members, business partners, etc.), educational institution, companies, funds, etc.
   6. Appeals
   7. Notes
      - Notations about people, not actionable
   8. Gifts
      - Gift type, subtype, date, amount, pledge schedule, campaign, fund, appeal, solicitors, payment method, acknowledgement/receipt info, etc., and in both a detailed and list format
   9. Attributes (for mailing)
   10. Media
   11. Actions
      - Notepad for actionable touchpoints with donors such as phone calls, letters, etc.
   12. Honor/Memorial (donations in memory of someone)
   13. Volunteer
   14. Prospects
      - Info about proposals and the prospective donors' capacity and inclination to give
   15. Membership
   16. Events – info about invitations to events and attendance

BBMS payment processing data includes: cardholder name, credit card number, expiration, CSC, and billing address.

Part 2 – Protection of Personal Information

In the following questions, delete the descriptive text and replace it with your own.

5. **Storage or Access outside Canada**

   As stipulated in the contract with Blackbaud, all data will be stored on Blackbaud cloud servers (Microsoft Azure) which is stored in Canada. Blackbaud confirmed this includes backup and failover data.

   The BBMS uses servers located in the United States.

6. **Data-linking Initiative***

In FIPPA, "data linking" and "data-linking initiative" are strictly defined. Answer the following questions to determine whether your initiative qualifies as a "data-linking initiative" under the Act. If you answer "yes" to all 3 questions, your initiative may be a data linking initiative and you must comply with specific requirements under the Act related to data-linking initiatives.	
1. Personal information from one database is linked or combined with personal information from another database;	NO
2. The purpose for the linkage is different from those for which the personal information in each database was originally obtained or compiled;	N/A
3. The data linking is occurring between either (1) two or more public bodies or (2) one or more public bodies and one or more agencies.	N/A
If you have answered "yes" to all three questions, please contact the privacy office(r) at privacy@ecuad.ca **to discuss the requirements of a data-linking initiative.**	

7. **Common or Integrated Program or Activity***

In FIPPA, "common or integrated program or activity" is strictly defined. Answer the following questions to determine whether your initiative qualifies as "a common or integrated program or activity" under the Act. If you answer "yes" to all 3 of these questions, you must comply with requirements under the Act for common or integrated programs and activities.	
1. This initiative involves a program or activity that provides a service (or services);	NO

2. Those services are provided through: (a) a public body and at least one other public body or agency working collaboratively to provide that service; or (b) one public body working on behalf of one or more other public bodies or agencies;	N/A	
3. The common or integrated program/activity is confirmed by written documentation that meets the requirements set out in the FOIPP regulation.	N/A	
Please check this box if this program involves a common or integrated program or activity based on your answers to the three questions above.	☐	

8. **Personal Information Flow Diagram and/or Personal Information Flow Table**

Personal Information Flow Table			
	Description/Purpose	**Type**	**FIPPA Authority**
1.	*ECU creates a backup file from the current Raiser's Edge production database located at ECU.*	*Use*	*32(a)*
2.	*ECU Systems transfers the database backup file via secure ftp to the secure file server at the new Blackbaud hosting environment*	*Use*	*32(a)*
3.	*Blackbaud restores the backup file to the new Raiser's Edge database server.*	*Use*	*32(a)*
4.	*To donate online: Donor enters and submits payment card information on ECU website (BBMS collects information to processes the payment. Payment information is not collected by ECU). Information includes:* - *First and last name;* - *Payment type and credit card number, expiry date, CVC;* - *Address, email, phone number;*	*Collection, Use, Disclosure*	*26(c), 32(a), 33.1(1)(i.1)*

-	*Donation amount and detail on what to support i.e. Scholarships; ECUAA graduating award; Emily Cares Fund; Other* - *Request for information of bequests*		
5.	*BBMS processes payment.*	*Use, Disclosure*	*32(a), 33.1(1)(i.1)*

9. **Risk Mitigation Table**

Risk Mitigation Table			
	Risk	**Mitigation Strategy**	**Likelihood**	**Impact**
1.	*Lack of legal authority to collection, use or disclose PI*	*Use of PI authorized by FIPPA and consistent with University programs and activities, will not be used for unauthorized purposes.*	*Low*	*High*
2.	*Unauthorized collection of PI by authorized individuals/processes/systems*	*Security read/write permissions limited on an account basis; password protection; where appropriate, consent is requested*	*Low*	*Med*
3.	*Excessive collection of PI by authorized individuals/processes/systems*	*Security read/write permissions limited on an account basis; staff only to collect relevant information for donor profiles; employee Code of Conduct*	*Low*	*Low*
4.	*Inappropriate or unauthorized use of PI by authorized individuals/processes/systems*	*Employee Code of Conduct, contractual terms; limited number of administrator/user seats (password protected); account security permissions are customized; contractual terms*	*Low*	*Low*

5.	*Unauthorized disclosure by individuals/processes/systems*	*Employee code of conduct, contractual terms, account security permission settings*	*Low*	*High*
6.	*Data stored outside of Canada and in the public cloud*	*Contractual terms (RE NXT); FIPPA authority (BBMS)*	*Low*	*Med*
7.	*Use of existing PI data in a new system or business process*	*Department is required to use information for consistent purposes as per FIPPA, new uses/collection of PI would require a PIA*	*Med*	*Med*
8.	*Unauthorized disclosure of payment card information by BBMS systems*	*BBMS encrypts personal and credit card information during all transactions; fraud mitigation provided by BBMS; industry-standard compliance including PCI-DSS and Certified SCO2 SSAE16 Type II data centres*	*Low*	*High*
9.	*Service provider privacy breach*	*Blackbaud has agreed in the Service Agreement to inform ECU within 72 hrs of security breach; a breach mitigation strategy will be developed with the Privacy Office*	*Low*	*High*

10. Collection Notice

RE NXT stores all data in Canada, therefore a collection notice regarding this transition is not necessary. Advancement fundraising activities themselves are out of scope for this PIA.

BBMS uses servers located in the United States. The university is authorized to disclose information outside of Canada under FIPPA [section 33.1(1)(i.1)](#):

(i.1) for the purposes of
    (i) a payment to be made to or by the government of British Columbia or a public body,
    (ii) authorizing, administering, processing, verifying or canceling such a payment, or
    (iii) resolving an issue regarding such a payment;

Facilitating a financial transaction using BBMS would be categorized under (i.1)(i) and (i.1)(ii). Therefore, consent in a prescribed manner is not required; donors will be notified that the payment is processed using Blackbaud.

Part 3 – Security of Personal Information

11. **Please describe the physical security measures related to the initiative (if applicable).**

Blackbaud enforces strict physical datacenter security based on best practices and SSAE18 audit guidelines:

All building entrances, the datacenter floor, and secure areas require card key access. The datacenter floor and secure areas also require two factor biometric authentication (hand/finger prints and iris scan).

Active patrol guards are onsite to monitor the interior and exterior of our facilities 24 hours a day, 365 days a year. We also have security cameras covering all entrances, alternate workspaces, and the datacenter floor.

12. **Please describe the technical security measures related to the initiative (if applicable).**

Blackbaud uses various strong encryption mechanisms across environments and products, including TLS 1.2, AES 256, RSA 1024 and other FIPS140-2 encryption algorithms.

Blackbaud ensures security of applications through constant education and training and routine vulnerability assessments.

As Blackbaud engages with Microsoft Azure, the details of security are covered at the Microsoft Azure Trust Center:
https://www.microsoft.com/en-us/trustcenter/cloudservices/azure
https://docs.microsoft.com/en-us/azure/security/azure-security-infrastructure

The responsibility and ownership of personal data lies with our business customers, per the Online Services Terms. However, Microsoft contractually commits that Azure and Intune in-scope services have implemented security safeguards to help them protect the privacy of individuals, based on established industry standards such as ISO/IEC 27001 and the SOC framework. We have assessed our practices in risk, security, and incident management; access control; data integrity protection; and other areas relative to the recommendations from the

Office of the Privacy Commissioner of Canada, and have determined that the in-scope services are capable of meeting those recommendations.

Azure continually monitors and updates their infrastructure security, more details can be found on their website: https://docs.microsoft.com/en-us/azure/security/azure-infrastructure-monitoring

RE NXT user accounts, roles and permissions are manually assigned by the administrator or department on a need-based basis. User access to the system is password protected and users must authenticate before accessing the platform. Users are limited to university staff within the Advancement + Events department.

13. **Does your branch/department rely on any security policies?**

    ECU employees are required abide by the Employee Code of Conduct and university policies, including:
    - 9.3 Code of Conduct for Appropriate Use of Information Technology, Facilities + Services
    - 9.4 Software Use + Copyright Compliance
    - 9.4.1 Software Use + Copyright Compliance Procedure
    - 9.6 Information Protection
    - 9.7 Laptop Security
    - 8.13 Confidentiality policy and procedure

    All university policies can be found online: https://www.ecuad.ca/about/leadership-and-governance/policies

    Questions around privacy and university policies can be directed to: privacy@ecuad.ca

14. **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.**

    Account management: ability to read/write will be restricted on an account-by-account basis based on need. Accounts are password protected. Changes and updates to donor profiles are completed by ECU staff.

15. **Please describe how you track who has access to the personal information.**

Access to data is limited to the users with accounts in the University Advancement + Events office.

<h2 style="background-color:#e6007e;color:white;">Part 4 – Accuracy, Correction + Retention of Personal Information</h2>

16. **How is an individual's information updated or corrected? If information is not updated or corrected (for physical, procedural or other reasons) please explain how it will be annotated? If personal information will be disclosed to others, how will the public body notify them of the update, correction or annotation?**

Depending on their security permissions, university employees can change/update personal information within the donor database to update donor profiles. Other users of the database will be able to access and view changes. Donors may contact the Advancement team to update the personal information in their profile, opt-out of communications (including those from Advancement, Alumni Relations, and regulation Communications newsletters), and/or delete their account.

17. **Does your initiative use personal information to make decisions that directly affect an individual(s)? If yes, please explain.**

Yes. The Advancement team will use personal information within the donor/individual profiles to support fundraising activities and strategy. This may affect the type and content of communications they receive from the university. Individuals on the platform may opt out of communications. Individuals on the platform may take action based on the communications if they wish (ie, donate).

18. **If you answered "yes" to question 17, please explain the efforts that will be made to ensure that the personal information is accurate and complete.**

The Advancement team will try to keep donor (individual) profiles accurate and up to date. Keeping accurate profile information is relevant to their fundraising activities. Users (university staff) will change and update personal information within individual profiles at the individual's request. Only university staff who have appropriate permissions within the system can make changes. Only university staff with access to the platform can view and access information.

19. If you answered "yes" to question 17, do you have a records retention and/or disposition schedule that will ensure that personal information is kept for at least one year after it is used in making a decision directly affecting an individual?

Donor/individual profiles within Raiser's Edge database are not automatically deleted on a schedule. A donor can choose to opt out of communications and/or request deletion of their account. Profiles and donation records are not deleted as to keep an ongoing record of donations and to affect later fundraising activities by the university.

Part 5 – Further Information

20. Does the initiative involve systematic disclosures of personal information? If yes, please explain.

For example: your department has a regular exchange of personal information (both collection and disclosure) with the federal government in order to provide services to your clients.

Please check this box if the related Information Sharing Agreement (ISA) is attached. If you require assistance completing an ISA, please contact your privacy office(r).	NO

21. Does the program involve access to personally identifiable information for research or statistical purposes? If yes, please explain.

For example: your public body will be disclosing information to PhD students so that they can conduct research.

Please check this box if the related Research Agreement (RA) is attached. If you require assistance completing an RA please contact your privacy office(r).	NO

22. Will a personal information bank (PIB) result from this initiative? If yes, please list the legislatively required descriptors listed in section 69 (6) of FIPPA. Under this same section, this information is required to be published in a public directory.

No.

Part 6 – Privacy Officer Comments

This PIA is based on a review of the material provided to the Privacy Office(r) as of the date below. If, in future any substantive changes are made to the scope of this PIA, the public body will have to complete a PIA Update and submit it to Privacy Office(r).

Audrey Chen

Privacy Office Representative

Signature

June 5, 2020

Date

Part 7 – Program Area Signatures
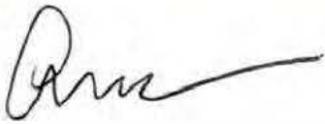
Chantale Lavoie		**June 5, 2020**
Program/Department Manager	Signature	Date
Sally Felkai		June 8, 2020
Contact responsible for Systems Maintenance and/or Security (Signature not required unless they have been involved in the PIA	Signature	Date
Adrian Tees		June 8, 2020
Head of Public Body (or designate)	Signature	Date

A final copy of this PIA (with all signatures) must be kept on record.

If you have any questions, please contact privacy@ecuad.ca or call the OCIO's Privacy and Access Helpline at 250 356-1851.