PIA # and Name- assigned by Privacy Office

1 General Information

1. Name of Department, Branch and Program Area

Lead-Financial Services, Treasury Services
Hospitality Services
Integrated University Planning on behalf of functional units for Salesforce TargetX CRM

2. Name of Program or Service Representative

Touchnet T-Link payment gateway - uPay

3. When will the initiative take place? 2/13/23

4. Is this a one-time event?

□ Yes ☑ No

5. Do you have an end date planned?

□ Yes ☑ No

6. Describe the New Program or Service or the Change.

Touchnet payment gateway (uPay) is used to collect payments for events, donations, workshops, youth camps, career fairs.

uPay can provide secure, PCI-compliant payment processing that moves campuswide payments into one centralized, certified system.

The payee would use our applications (for example: TargetX and SeattleTech Iris Coordinator) to register for an event there would be a "Pay Now" button on the page that the Touchnet t-link connection pushes the person to the Touchnet Marketplace dashboard to enter in their name, credit card information. Once payment is made and approved a prompt "payment confirmation" is sent back into our application and triggers to mark as paid.

7. Describe the Purposes, Goals and Objectives.

The purpose of integrating a payment gateway with the Salesforce CRM, TargetX application and Seattle Technologies is to collect payments from clients by credit card for event fees, donations, fundraising, youth camps, fees for career fairs, craft fairs.

8. Describe the Governance Model – who is ultimately accountable for the program or system.

-The UNBC Financial Services, Treasury Services Manager, is accountable for the payment gateway account and for setting up the admin users who access the system.
-ITS CRM Technical Administrator is accountable to configure and maintain the payment connector in the CRM's system and monitor that proper event procedures are adhered to.
-UNBC Unit leads using the payment feature in the CRM are responsible to reconcile event payments through uPay platform.

9. List any Relevant PIAs

Salesfore
Touchnet ID Card

10. List of All Stakeholders Impacted / Involved (i.e. who are you collecting information from, UNBC roles using PI, 3rd parties with whom you will share information)

Stakeholder	Role in the initiative
Clients (UNBC members and non-UNBC members)	accessing the Touchnet payment gateway to make payments using their credit card information
UNBC departments	view client information to reconcile payments and refunds
UNBC Finance	Set up of payment gateway account with vendor
UNBC ITS (CRM Technical Administrator)	Configure and maintain the payment gateway/connector in the CRM
CRM Oversight Committee	Oversee the governance of the CRM

11. List any relevant contracts or software purchases. Be sure to follow UNBC guidelines regarding purchasing policies.

TouchNet

2 Collection and Use of Personal Information

12. What are the data or information elements involved in your initiative?

Data Element name, email, id#, grade	Rationale for collection, use or disclosure	Method of Collection or Disclosure	FIPPA Section (completed by Privacy)
Credit/debit card notification	Touchnet uPay will process payments UNBC will receive notification of payment, not credit card information.	Direct [✓ Indirect]	26(c)
Name of payee	To reconcile payments with the payee	[✓ Direct] Indirect	26(c)
Email of payee	To send a confirmation of payment email	[✓ Direct] Indirect	26(c)
Address of payee	To complete the payment transaction	[✓ Direct] Indirect	26(c)
credit card info	Over the phone to assist with payment for an event.	[✓ Direct] Indirect	26(c)
		Direct [✓ Indirect]	TBD
		Direct [✓ Indirect]	TBD

13. Describe how personal information is to be collected

-Touchnet uPay: end user enters information through text fields on the uPay site

-Salesforce CRM: personal information collected use applications such asTargetX. Credit card information is not collected in the CRM. Unit users using TouchNet uPay for CRM related events must refer clients to the TouchNet uPay site to make payments.

-Hospitality Services: Registrant calls a UNBC Department such as Hospitality Services to register and pay for an event. Personal data is entered on their behalf (while they are on the phone).

14. If you already have a collection notice, attach it as an appendix.

15. Please list all users of PI and Describe how personal information is to be used.

User (UNBC Roles e.g Governance officer)	How the info is used
Hospitality Services Staff (supporting over the phone payment)	Registrant calls to register and pay for an event. Personal data is entered on their behalf (while they are on the phone).
Hospitality Services Staff	will have access to Touchnet to generate transaction reports that include: Date, Time, Amount, Transaction#, etc... but will not receive credit card information.
UNBC authorized users using SalesForce Apps	will view transaction details such as date, time, $ amount, but will not access credit card information directly.
Finance Staff	will access the TouchNet uPay site to generate transaction reports needed for the reconciliation of payments and refunds

16. Do you use personal information in your initiative to make a decision about an individual?

☑ Yes ☐ No

17. If yes, do you have a retention schedule in place related to personal information used to make decisions?

☐ Yes ☑ No

18. If yes, please your approved information schedule as an appendix.

19. If you answered no, describe how you will ensure the information will be kept for a minimum of one year after it's used to make a decision that directly affects an individual.

All UNBC units collecting payment information from Touchnet Payment Gateway are required to work with Access, Privacy, and Records Management in order to have an approved retention schedule with the first year of data collection.

3 Storage of Personal Information

20. Is any personal information stored outside of Canada?

☑ Yes ☐ No

21. Describe how PI information will be stored

For example, are you using a cloud storage (OneDrive), or Software as a Service (SaaS).

[redacted]

22. Does your initiative involve digital tools, databases information systems?

☑ Yes ☐ No

If yes, please discuss with UNBC Information Security whether you also require a security and threat risk assessment

4 Research / Health System Use

23. Do you anticipate that data collected by this program / system will be used for research or health system use?

□ Yes ☑ No

If "Yes" answer the following questions, if“No” please proceed to the next section.

24. Please explain and provide details of data state (aggregate, de-identified, anonymized etc.)

NA

25. Will it be disclosed as part of Health System Use?

Provide details on the disclosure, including where and how personal information will be stored.

NA

26. Will it be disclosed as part of Research / Open Data?

Provide details on the disclosure, including where and how personal information will be stored.

NA

5 Disclosure

27. Will you be disclosing information to 3rd parties (i.e. non-unbc employees?

☐ Yes ☑ No

If "Yes" answer the following questions, if "No" please proceed to the next section.

28. To whom will you be disclosing personal information?Provide details on the disclosure, including where and how personal information will be stored.

NA

29. If personal information will be disclosed to anyone outside of Canada, provide details on the disclosure,including where and how personal information will be stored.

NA

6 Accuracy and Correction

30. How will you make sure that the personal information collected is accurate and complete?

The end user inputs their own information directly to Touchnet uPay. UNBC authorized users are not inputting personal information. Only the payee can ensure personal information is accurate and complete.

31. Do you have a process in place to correct personal information?

☑ Yes □ No

32. If yes, please describe your process below?

An error message indicating incorrect information is displayed and the payee must correct the information before moving forward with payment.

If a payment is reported as incomplete, the registration software system (ie: Salesforce, Target X) that is linked to Touchnet will report an error to the UNBC authorized user. UNBC can notify the end user that their registration was not processed and they can try again.

33. Describe the process of how you will make a note on the record, if you're not able to correct the record itself.

NA

34. If you receive a request for correction from an individual and you know you disclosed their personal information in the last year, FOIPPA requires you to notify the other public body or third-party recipient of the request for correction. How will you ensure that you conduct these notifications when necessary?

No 3rd Party disclosure identified for this initiative, not process for 3rd party notification of FOI required

7 Personal Information Banks

A personal information bank is a collection of personal information that is organized or searchable by the name of the individual or an identifying number, symbol, or other identifier. A personal information bank can be a simple list of personal information. Personal information banks contain personal information that is:

- linked to an identifiable individual
- organized and capable of being retrieved by a personal identifier
- normally compiled for a single purpose

35. Will your initiative result in a personal information bank?

□ Yes ☑ No

If "Yes", answer the following questions, if "No" please proceed to the next section.

36. Describe the business purpose for the information bank (i.e., account management of clients, student record management)

Touchnet payment gateway (uPay) is used to collect payments for events, donations, workshops, youth camps, career fairs.

37. If aggregate reports are generated, explain how Personal Information will be de identified or anonymized and by whom?

38. Describe the category of users and the information to which they will have access

Category of Users	Information accessed (i.e. contact info, grades, fee etc.)
To be defined before use of system	To be defined before use of system

39. Who is responsible for oversight of user access?

Treasury Services Manager

40. Who reads the audit logs, and how long are they kept?

[redacted]

41. What does the audit log track? How detailed is the data (e.g., date stamps, time stamps, access control number, IP address, etc.)? Does the audit log include the purpose of an access?

To be defined by end of 2023-24 fiscal year

42. Are the audit logs immutable?

□ Yes □ No

43. Is there a separation of responsibility between those who supervise administration of the system, or security of the system, and those who verify the audit logs (e.g., does the auditor in the organization have a role, or is it the security department?)

[redacted] Yes [redacted] No

44. Is the system responsive or passive? For instance, is it possible to put a monitor on particular individuals (e.g., in a hospital setting, if a celebrity is admitted as a patient, etc.)? Will access produce an immediate response and not just a log entry for review months later?

To be defined by end of 2023-24 fiscal year

45. How will those found to abuse access privileges be sanctioned ?

To be defined by end of 2023-24 fiscal year

8 Privacy and Security Safeguards

46. Describe administrative safeguards (i.e. policy documents, procedures, or training).

[redacted]

47. Describe physical safeguards (i.e. locked, filing cabinets, locked doors, or restricted areas).

[redacted]

48. Describe the controls in place to prevent unauthorized access to personal information (i.e. role-based access to software, access logs).

[redacted]

49. Describe technical safeguards (i.e. firewalls, encryption, or intrusion prevention systems).

[redacted]

9 Privacy Risk Identification and Mitigation

50. Identify any privacy risks, even very unlikely ones, associated with the initiative and the mitigation strategies that will be implemented (see risk classification table).

Try to include at least one risk related to each step is the information cycle (collection, storage,access, disclosure, and destruction. **If you are disclosing or storing data outside of Canada you will need to identify additional risks related to storage/disclosure outside of Canada**

RISK	LIKELIHOOD	IMPACT	MITIGATION STRATEGY
[redacted]			

RISK	LIKELIHOOD	IMPACT	MITIGATION STRATEGY
[redacted]	[redacted]	[redacted]	[redacted]
	[✓ Low] Moderate High	[✓ Low] Moderate High	
	[✓ Low] Moderate High	[✓ Low] Moderate High	

10 Data Linking

In FOIPPA, “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.

51. Does this initiative involve a program or activity that provides a service(s) through a public body and at least one other public body or agency working collaboratively to provide that service?

□ Yes ☑ No

52. Does this initiative involve a program or activity that provides a service(s) through a public body that is working on behalf of one or more other public bodies or agencies?

□ Yes ☑ No

53.The common or integrated program/activity is confirmed by written documentation that meets the requirements set out in the Regulations? (Privacy Officer will answer).

□ Yes ☑ No

If this PIA addresses a common or integrated program, UNBC must submit this PIA to the Office of the Information and Privacy Commissioner and be subject to their examination, advice, and timelines.

11 Conclusions and Approvals

Individual leading the Program/Project:

Position:

I confirm the information management practices in this initiative have been documented as accurately as I am aware. I commit to communicating appropriate information management practices to all individuals participating in this initiative. I commit to following the documented practices on this PIA, or arranging a PIA amendment if I am aware information management practices in this initiative change.

Signature:_[redacted]_____________________Date:_August 16, 2023_

Director/Dean Overseeing the Program/Project:

I am accountable for overseeing my staff involved in this initiative to ensure they adhere to information management practices presented in this PIA. I will arrange for the project lead named above to contact the Privacy Officer to arrange a PIA amendment if required.

Signature:_[redacted]_____________________Date:_Aug 17/23_

Name of Vice-President

I confirm that this initiative to the best of my knowledge as written in the above sections,has information management practices that complies with policies and procedures of the University of Northern British Columbia.

Signature:_[redacted]_Kiran Kullar Acting on Rahim Somani's behalf_Date:_Aug 17/23._

Name of Privacy Officer: Christopher Ross

I confirm that this initiative to the best of my knowledge as written in the above sections, has information management practices that comply with British Columbia's Freedom of Information and Protection of Privacy Act.

Signature[redacted]_____________________Date:_August 25, 2023_

General Policy

The University of Northern British Columbia (UNBC) collects and processes information in compliance with the **BC Freedom of Information and Protection of Privacy Act (FOIPPA).** For online payments for events, youth camps, vendor fairs, and donations, customer information is collected and limited to those details necessary to process your payment. This includes personal information (student/donor identification) and financial information (credit card number, expiry date). This information is being collected by UNBC under FOIPPA 26(c).

Credit card information is not stored by the University of Northern British Columbia. It is collected to authorize and process the payment by TouchNet, our payment gateway provider. Security measures have been integrated into the day-to-day operating practices of the University. For more information on the University's terms and privacy policies, please refer to http://www.unbc.ca/policy/category/foipop.html. If you have questions regarding the security of your information, please contact finance@unbc.ca.

When you are finished conducting online transactions or visiting secure web sites, remember to properly log-off and close your browser. This will ensure that any information that is stored on your computer or in your browser is erased. This will prevent others from being able to view this information later.

Refund Policy

Requests for refund can be submitted to finance@unbc.ca.

By clicking the Submit button below you indicate that you agree to and have read the Terms & Conditions and Privacy Policy.

Accept Terms You will then be forwarded to the TouchNet uPay web-site for payment and will then be returned to the UNBC web-site. The navigation will appear seamless. You will receive an email payment notification from TouchNet uPay. Please enter a valid email address for payment notification.

Available payment options will be listed on the payment site.

13 Key Terms

"**personal information**"means recorded information about an identifiable individual, including,

(a) information relating to the race, national or ethnic origin, colour, religion, age, sex, sexual orientation or marital or family status of the individual,

(b) information relating to the education or the medical, psychiatric,psychological, criminal or employment history of the individual or information relating to financial transactions in which the individual has been involved,

(c) any identifying number, symbol or other particular assigned to the individual,

(d) the address, telephone number, fingerprints or blood type of the individual,

(e) the personal opinions or views of the individual except where they relate to another individual,

(f) correspondence sent to an institution by the individual that is implicitly or explicitly of a private or confidential nature,and replies to that correspondence that would reveal the contents of the original correspondence,

(h) the individual's name where it appears with other personal information relating to the individual or where the disclosure of the name would reveal other personal information about the individual.

Risk Classification Table

***Risk Levels**	**Likelihood**	**Harm**
Low	Little possibility that the risk will occur due to mitigating factors	Compromise would likely not result in any significant harm to the privacy, safety, or economic standing of individuals or the corporation.
Moderate	A possibility that the risk will occur if no additional measures are taken.	Compromise would likely cause some harm to the privacy, safety, or economic standing of individuals or the corporation.
High	Near certainty that the risk will occur in the future if no corrective measures are taken.	Compromise would likely cause significant and immediate harm to the privacy, safety, or economic standing of individuals or the corporation.