Privacy Impact Assessment (PIA)

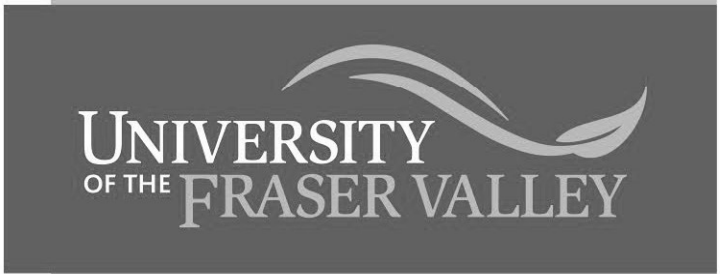
Version 0.3e

iCent Service

Program Manager:
xxxxxx
Director of Infrastructure and Operations,
Office of the Chief Information Officer

Author:
Crawford Millen
Security Architect
Office of the Chief Information Officer

Date:
2021-03-10



Version History

Ver	Date	Author	Description
0.1	2021-02-09	s. 22	s. 22
0.2	2021-03-04		
0.3	2021-04-12		
0.4			
0.5			
0.6			
0.7			
0.8			
0.9			
1.0			
1.0b			

Table of Contents

Part 1 – General

Name of Department/Branch:	Crawford Millen		
PIA Drafter:	Crawford Millen		
Email:	Crawford.millen@ufv.ca		
Program Manager:			
Email:			

The objective of a Privacy Impact Assessment (PIA) is to determine how a program or service, could affect the privacy of individuals. It aims to identify and reduce any possible negative effects on privacy that might result from implementing a program or service. This specific PIA's objectives are first to determine if there are privacy issues or risks associated with the University of the Fraser Valley's proposed use of the iCent service; and if so, to provide recommendations and mitigation strategies. This will include identification of issues with compliance with regard to the *Freedom of Information and Protection of Privacy Act,* R.S.B.C. 1996, c. 165 ("FIPPA"), and determine how UFV can avoid or minimize the loss, damage, misuse or abuse of personal information.

In addition, this PIA is a way for UFV to demonstrate its commitment to protecting the privacy of individuals, promote transparency and accountability, and contribute to continued public confidence in the way that the University of the Fraser Valley (UFV) manages personal information. It helps prepare UFV to implement the project with proper consideration of relevant privacy requirements, including those privacy requirements in the architecture, design, and configuration.

This PIA is guided by the requirements laid out in FIPPA:

Section 69(5.3) of the Freedom of Information and Protection of Privacy Act (FIPPA) requires the head of a public body to conduct a privacy impact assessment (PIA) in accordance with the directions of the minister responsible for FIPPA. Public bodies should contact the privacy office(r) for their public body to determine internal policies for review and sign-off of the PIA. Public bodies may submit PIAs to the Office of the Information and Privacy Commissioner for BC (OIPC) for review and comment.

This PIA also explains the process UFV followed, the factors considered, and the steps taken or will undertake to make sure this decision does not adversely affect the privacy of the UFV community. This undertaking is part of UFVs commitment to make careful and considered decisions in safeguarding the personal information of staff, students, and all other stakeholders. It explains our reasons for the move, the context within which we made the decision, the key privacy risks identified as potential barriers to cloud use, and the reasons these can be overcome.

This report is meant to aid information technology, information management, and access to information and privacy staff, along with the directors and executive directors, to be better informed about the risks, and recommend appropriate safeguards in order to securely transition to the cloud.

1. Description of the Initiative

The use of the iCent app to provide 24/7 remote assistance to international students schedule to begin their studies at UFV, including returning students. The app includes content that provides students with local, provincial and federal Covid-19 guidelines, institutional level information, as well as advice from public health authorities. The information provided also includes instructions to international students about any applicable quarantine obligations (under the Quarantine Act) and their mandated COVID-19 test. The app includes a detailed pre-arrival guide, self-serve tools, links to on-campus support, and post-arrival guide and more.

2. Scope of this PIA

iCent is a custom-branded app which functions as an international student acclimatization tool. It provides international students with pre and post-arrival checklists, information about health insurance, local transportation, banking and shopping and other aspects of life in Canada. The version that is being made available to UFV students will be integrated with the student's guard.me international insurance policy. The app provides a mechanism to provide international students with information about COVID-19 travel restrictions and quarantine requirements. Many students do not open email messages in a timely fashion and this app enables UFV to send "push" notifications to students who have downloaded and use the app – providing UFV International staff with an additional means of communication with students.

The iCent tool will also provide a convenient method for UFV to provide information to international students.

3. Related Privacy Impact Assessments

s. 21, s. 15(1)(l)

4. Elements of Information or Data

The following is summary of the personal information collected using the app:

- Emergency Contact: Contact's Name, phone number, relationship, email address, home address;
- Quarantine Plan: name, student number, preferred email, phone number, flight itinerary, whether they are a new or returning student, whether or not they are new to Canada, quarantine location, and details about quarantine location (i.e. hotel, staying with family or friends), other details about their quarantine (such as whether they know how to order food to their quarantine location).
- A confirmation will be collected at the conclusion of the quarantine and the student will confirm the test results of their final COVID test

In addition to the above, Neel-Tech states that it collects non-identifying information such as the user's IP address, browser type, access times, domain names, and usage information while using the app. This information would not necessarily be considered to be personal information on its own but when combined with other information that could identify an individual is likely to also be considered personal information.

If personal information is involved in your initiative, please continue to the next page to complete your PIA.

If no personal information is involved, please submit Parts 1, 6, and 7 to your privacy office(r). They will guide you through the completion of your PIA.

Part 2 – Protection of Personal Information

5. Storage or Access outside Canada

Storage

s. 15(1)(l), s. 21 [redacted]

Access

s. 15(1)(l), s. 21 [redacted]

6. Data Linking Initiative

In FOIPPA, "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;	NO
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.	NO
If you have answered "yes" to all three questions, please contact your privacy office(r) to discuss the requirements of a data-linking initiative.	

7. Common or Integrated Program or Activity

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.	
1. This initiative involves a program or activity that provides a service (or services);	**NO**
2. Those services are provided through: (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;	**NO**
3. The common or integrated program/activity is confirmed by written documentation that meets the requirements set out in the FOIPP regulation.	**NO**
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 – Typical student use			
#	**Description/Purpose**	**Type**	**FIPPA**
1	Student becomes aware of the app services via UFV International and downloads the iCent app from Google Play, Apple App Store or a direct link from the iCent web site;	N/A	N/A
2	Student creates a user account with iCent and provides personal information required to use the service	Information Collection	26(c)
3	Student information gathered during processing for iCent services. It is possible, for example, that a student could connect with UFV via the app to arrange airport pickup arrangements or similar services, however, it is not anticipated that UFV will use this capability.	Information Use	32(a)

9. Risk Mitigation Table

Risk	Prob-ability	Impact	Neel-Tech Measure	UFV Measures
s. 15(1)(l), s. 17	Low	High	s. 15(1)(l), s. 17, s. 21	s. 15(1)(l), s. 17
s. 15(1)(l), s. 17	Low	High	s. 15(1)(l), s. 17, s. 21	s. 15(1)(l), s. 17

Risk	Prob-ability	Impact	Neel-Tech Measure	UFV Measures
Data in transit may get compromised	Medium		s. 15(1)(l), s. 17, s. 21	Cybersecurity review has to completed by UFV to ensure Neel-Tech measures are as stated.
Data at rest may get compromised	Low	High	s. 15(1)(l), s. 17, s. 21	Contractual provisions regarding security of data at rest between UFV and vendor. s. 15(1)(l), s. data centre certifications are renewed periodically, and include review of physical and process controls.

Risk	Prob-ability	Impact	Neel-Tech Measure	UFV Measures
Compromise of a user's Authentication credentials	Low	High	s. 15(1)(l), s. 17, s. 21 [redacted]	Cybersecurity review has to completed by UFV to ensure Neel-Tech measures are as stated.
Excessive collection of PI	Low	High	Service can be configured to collect only the information required by UFV and is in alignment with privacy laws.	UFV can configure the iCent tool to collect only the information required for the iCent service to be used to deliver UFV services

10. Collection Notice

Collection Notice: Personal information collected using the iCent app is collected by the University of the Fraser Valley under the authority of section 26 (c) of the *Freedom of Information and Protection of Privacy* Act. Information collected will be shared with UFV's International office for the purpose of providing international office services and information to students. If you have any questions about this collection of personal information please contact UFV's international office at international@ufv.ca.

Part 3 – Security of Personal Information

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

s. 15(1)(l), s. 17, s. 21

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

s. 15(1)(l), s. 17, s. 21 [redacted]

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

Not Applicable

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.

s. 15(1)(l), s. 17, s. 21 [redacted]

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

s. 15(1)(l), s. 17, s. 21 [redacted]

Part 4 – Accuracy/Correction/Retention of Personal Information

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?

Students are in control of their own information, they have access to update/change their information by login in to their iCent profile.

Likewise, UFV personnel also have access to, either update the student info based on enrolment data and/or notify the student via notifications to update the information.

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

No

18. If you answered "yes" to question 16, please explain the efforts that will be made to ensure that the personal information is accurate and complete.

N/A

19. If you answered "yes" to question 17, do you have 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?

N/A

Part 5 – Further Information

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

No

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).	

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

Not Applicable.

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).	

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 FOIPPA. Under this same section, this information is required to be published in a public directory.

Not Applicable.

Please ensure Parts 6 and 7 are attached to your submitted PIA.

Part 6 – Privacy Office(r)/or individual responsible 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 the Privacy Office(r).

Stephen Gaspar Legal Counsel University of the Fraser Valley	Signature	Date

Part 7 – Administrative Office(r)/or individual responsible comments

This PIA is based on a review of the material provided to the Administration 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 the Administrative Office(r).

Jackie Hogan Chief Financial Officer & VP Administration, University of the Fraser Valley	Signature	Date

Part 8 – Program Area Signatures

Steven Banyai Chief Information Officer, University of the Fraser Valley	Signature	Date
Crawford Millen Author/Director Information Security OCIO University of the Fraser Valley	Signature	Date
Jacqueline Toering Dir. Risk & Safety, University of the Fraser Valley	Signature	Date
Alex Diaz Dir. Infrastructure & Operations OCIO, University of the Fraser Valley	Signature	Date

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