A GUIDE TO THE COMPLETION OF A PRIVACY IMPACT ASSESSMENT (PIA)

What is a PIA?

A PIA is a privacy risk assessment tool that is used in identifying and assessing privacy related impacts for any system/program/legislation which collects, uses, discloses, and/or secures personal information. A PIA is also used when a change occurs to an existing system/program/legislation that collects, uses, discloses and/or secures personal information.

Why Complete a PIA?

PIA's are a legal requirement for all public bodies under S.69 (5.3) of the *Freedom of Information and Protection of Privacy Act* (*FIPPA*). In addition to being a legal requirement, PIA's act as an "early warning system" by identifying deficiencies with regards to privacy protection. It can assist management in making informed decisions and avoid privacy breaches by ensuring an organization is complying with *FIPPA*. The PIA demonstrates accountability by including privacy as part of the design of new initiatives or systems. When designing a new initiative or program with privacy in mind, unnecessary costs are avoided throughout the process as it is inclusive from the beginning. Initiatives cannot proceed to implementation without completion and formal signoff of a PIA.

When to Complete a PIA?

PIA's should be drafted during the initial development stage of any new system/program/legislation. PIA's should also be drafted for *amendments* to existing programs/systems/legislation that detail the privacy impacts of the changes. In many circumstances, the PIA is an evolving document that becomes more detailed over time as the initiative progresses.

If the initiative involves data-linking or a common or integrated program or activity, as defined by *FIPPA,* the Office of the Information and Privacy Commissioner of British Columbia (OIPC) must be notified at an early stage in the development of the document by UFV's Privacy Consultant.

The PIA must be completed and signed off prior to the implementation of a new initiative or "launch" date of a new system or program.

Who is Responsible for a PIA:

PIA's should be drafted by the program area project manager responsible for the implementation of the system/program/legislation. Program area managers are responsible for the approval of the PIA ensuring compliance with *FIPPA* before implementation. In developing a PIA, the project manager must work closely with both Legal Counsel and the Information Technology Department.

How to Write a PIA:

The Province of British Columbia provides a template for the writing a PIA:
http://www2.gov.bc.ca/gov/content/governments/services-for-government/information-management-technology/privacy/privacy-impact-assessments

If you have any questions regarding the completion of a PIA, please contact Maureen Murphy, UFV Legal Counsel, at 604-854-4572 or Maureen.murphy@ufv.ca.

UNIVERSITY OF THE FRASER VALLEY

Part 1 – General

Name of Department/Branch:	Financial Services		
PIA Drafter:	Deanna Stelting		
Email:	Deanna.stelting@ufv.ca	Phone:	604-854-4512
Program Manager:			
Email:		Phone:	

This section includes the name of the department/branch of the organization, drafter of the PIA, the program manager and their respective contact information (eg. Email/Phone). This information is especially important if the PIA will be reviewed by external stakeholders. The program manager must be able to respond to detailed questions regarding the PIA.

1. Description of the Initiative

This is a new online initiative that is inline with the university's policy #235, Travel Approval, Booking and Reimbursement. This ongoing initiative, a centralized travel booking service, will collect personal information to facilitate the booking of travel (air, hotel, car). The personal information is stored in the United States by Trondent, the provider of the profile software used by Uniglobe. For international travel, personal information is shared between Trondent and International SOS, at time of booking, which may store the information in the United States.

2. Scope of this PIA

This PIA will review all aspects of the online system from Uniglobe to Trondent and then further with Trondent to International SOS.

3. Related Privacy Impact Assessments

This is a new initiative.

4. Elements of Information or Data

The following personal information is collected as part of the traveller profile:

- Name
- Date of birth
- Gender
- Home phone number
- Home Address
- Passport Number
- Nexus Number (

As part of International SOS, the following information may be collected:

- Full Name
- Address
- Telephone number
- Email address
- Gender
- Date of Birth
- Nationality
- Family Status

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

Personal information will be stored by Trondent in s. 15(1)(l), s. 17

Personal information may also be stored in the United States by International SOS.

Consent for sharing traveler's personal information will be obtained in advance. If consent is not given, the traveler must contact the Financial Services department.

UNIVERSITY OF THE FRASER VALLEY

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;	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 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);	YES
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;	NO
3. The common or integrated program/activity is confirmed by written documentation that meets the requirements set out in the FOIPP regulation.	NA
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

The PIA must provide a clear picture of how the personal information data flows, who has access to it and for what purpose. Include a narrative description of the data flows and/or a schematic/chart illustrating the process of collection/use/disclosure of personal information.

Personal Information Flow Table			
	Description/Purpose	**Type**	**FIPPA Authority**
Describe each step of the information flows detailed above and list numerically. Determine if each step represents collection, use, and/or disclosure of the personal information (examples below).		*Is this collection, use or disclosure?*	*Cite section of the FIPPA that provides authority*
Trondent			
1.	Individual registers, creates password and profile	Collection	
2.	Individual creates travel reservation (air, hotel, car) online or by phoning a Uniglobe travel agent	Use	
International SOS			
1.	Travel reservation information (air, hotel, car) shared with International SOS	Disclosure	
2.	Booking information used to monitor travel situations	Use	

9. Risk Mitigation Table

Risk Mitigation Table				
	Risk	**Mitigation Strategy**	**Likelihood**	**Impact**
Trondent				
1.	Unauthorized access of a profile	s. 15(1)(l), s. 17	Low	High
2.	Server where profile information is stored is hacked	[redacted]	Low	High
3.	Personal information is stored in the United States and is subject to the Patriot Act.	s. 15(1)(l), s. 17	Low	High
International SOS				
1.	Unauthorized access of profile information	s. 15(1)(l), s. 17	Low	High

2.	Server where profile information is stored is hacked	[redacted]		
3.	Personal information may be stored in the United States and is subject to the Patriot Act	s. 15(1)(l), s. 17 [redacted]		

10. Collection Notice

Provide the notification clause/language that individuals must be provided with prior to submitting their personal information. The clause must reference the authority under which the public body operates as well as FIPPA, the purpose for collection/use/disclosure of the personal information and the position/email address and physical address of a contact position that can speak to the privacy implications of the initiative. References to the method of collection, an organization's privacy policies and supporting documentation may also be included.

Part 3 – Security of Personal Information

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

Per the Trondent Security and Data Privacy Guidelines, the following is used for physical security

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

Per International SOS privacy policy, the following is used for physical security:

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

.

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

Per the Trondent Security and Data Privacy Guidelines, the technical security measures are as follows:

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

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

Per the International SOS privacy policy, the following is used:

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

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

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

Trondent has the *Security and Data Privacy Guidelines* which outlines in detail the security policies adhered to by all employees at the company.

International SOS:
s. 15(1)(l), s. 17 [redacted]

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 [redacted]

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

s. 15(1)(l), s. 17 [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?**

It is up to the traveller to ensure their personal information is kept current and correct. This information is stored in Profiler Express, an online tool used by Trondent for the management of the personal information.

Travelers will have access to their profile through International SOS where they will be able to manage their personal 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 17, 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

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

    Yes. At the time of booking travel, personal information along with booking ifnromation will be shared between Trondent and International SOS.

Please check this box if the related Information Sharing Agreement (ISA) is attached. If you require assistance completing an ISA, please contact UFV's legal counsel.	

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

    No

Please check this box if the related Research Agreement (RA) is attached. If you require assistance completing an RA please contact UFV's legal counsel.	

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

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

Part 6 – UFV's legal counsel /or individual responsible comments

This PIA is based on a review of the material provided to UFV's legal counsel 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 UFV's legal counsel.

Maureen Murphy, Legal Counsel, University of the Fraser Valley	Signature	Date

Part 7 – Program Area Signatures

Insert name of Program/project manager responsible. Department University of the Fraser Valley	Signature	Date
(insert name of contact responsible for information systems), Systems Maintenance and/or Security (Signature not required unless they have been involved in this PIA.) University of the Fraser Valley	Signature	Date
(insert name of Chief Information officer) University of the Fraser Valley	Signature	Date
Head of Public Body, or designate University of the Fraser Valley	Signature	Date

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