Royal Roads
UNIVERSITY

Royal Roads University
Privacy Impact Assessment
International SOS (ISOS)

Part 1 – General

Name of Department/Branch:	RRU - Financial Services		
PIA Drafter:	Hooper Access and Privacy Consulting Ltd.		
Email:	bev@hooperconsulting.ca	Phone:	(250) 896-4272
Program Manager:	Jessica Subin, Associate Director, Financial Services		
Email:	Jessica.Subin@RoyalRoads.ca	Phone:	250 391-2600 ext 4415

1. Description of the Initiative

The Canadian Trade Commissioner Service of the Government of Canada recommends that employers consider risks to individuals while on travel status and take steps to ensure that due diligence and practical standards are met. This includes development of a corporate policy (eg. Risk assessment, response planning, incident management, etc.) for international travel.

Under the Criminal Code of Canada, organizations are responsible for providing 'Duty of Care' and "reasonable steps" to protect individuals whether in Canada or internationally. If an organization does not meet this Duty of Care requirement, they can be found criminally and financially liable.

Royal Roads University (RRU) has developed a travel management program to ensure Duty of Care and employee/student safety while on travel status to comply with federal recommendations and obligations. The program includes assessment of risk to the individual while travelling, strategies and planning to address any risks to the traveller, policies and procedures, emergency management, awareness and training and employee/student tracking.

As part of this initiative, the International SOS (ISOS) System has been implemented to ensure the security and safety of individuals while on travel status.

ISOS provides medical/clinical/security advice and assistance to organizations with international travellers and/or operations. Services include planning and preventative programs, travel advisories, providing potential risks to travellers, in-country expertise and emergency response. ISOS is a private company and provides support in 89 countries.

Bookings for international travel for employees/students are completed by the traveller or a designated RRU Travel Counsellor. The traveller has to upload their travel itinerary information to the ISOS system. As part of the ISOS service, a report is generated and provided is to Associate Vice President, Financial Services and Associate Vice President, Operations and Resilience.

The ISOS system reports on safety incidents occurring internationally (eg. natural disasters, acts of terrorism, etc.) and whether there are travellers from RRU in areas with raised profiles for incidents. This information is also used to inform the approval of travel based on current/potential risks (eg. crime, illness, terrorism, safety hazards, civil unrest, etc).

In the event of a medical emergency or safety incident, ISOS will formally notify RRU by email/telephone which will identify the traveller, risk and care options available.

RRU is committed to ensuring that this project meets privacy and security policies and practices, and will manage the privacy risks associated with legislative requirements accordingly. ISOS privacy risks are managed through a combination of technical, administrative and physical controls that mitigate the associated risk. RRU has a dedicated privacy officer, supporting privacy policies/procedures and provides employee training. This privacy impact assessment (PIA) is intended to ensure that this program is offered in a way that is compliant with the *Freedom of Information and Protection of Privacy Act* (FIPPA).

2. Scope of this PIA

This Privacy Impact Assessment (PIA) details the collection, use, disclosure and security of personal information provided by employees and students in support of the use of ISOS.

3. Related Privacy Impact Assessments

No previous PIA's have been completed related to this initiative.

4. Elements of Information or Data

The following personal information is collected by ISOS at the time the individual provides travel information:

Mandatory Fields (ISOS travel tracker site):

- First/Last Name
- Email Address
- Country of Origin
- Travel Itinerary Information

Optional Fields (*provided at traveller's discretion)

- Primary Telephone Number

Part 2 – Protection of Personal Information

5. Storage or Access outside Canada

ISOS stores client data on servers in Canada (Toronto), USA (Philadelphia, Dallas) and the United Kingdom (London). ISOS employs comprehensive Data Protection, Information Security, Retention, Archiving and

Destruction Policies governing the collection, security, disclosure and legal compliance when managing personal information.

Users are notified upon collection of personal information that the PI will be stored and accessed by a third party service provider (ISOS) outside of Canada for the sole purpose of providing out-of-country safety and security purposes.

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);	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.	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 Table			
	Description/Purpose	**Type**	**FOIPPA Authority**
1.	Personal information is disclosed to ISOS by the traveller to populate the ISOS system.	Use	*32(a)*
2.	Personal information is provided to RRU by ISOS to provide travel information and allow for notification of global safety incidents.	Use	*32(a)*
3.	ISOS provides traveller with notification details to assist traveller with risk mitigation.	Use	*32(a)(b)*

9. Risk Mitigation Table

Risk Mitigation Table				
	Risk	**Mitigation Strategy**	**Likelihood**	**Impact**
1.	Unauthorized individuals could access the personal information in the system and use or disclose it for personal purposes (within RRU).	Limited user access based on need to know for operational purposes only. Password protected sign in to access personal information in the system, user access to reports and dashboards assigned appropriately, permissions restricted and monitored. All employees are required to abide by RRU's privacy policies and guidelines.	Low	High
2.	User's personal information is accessed externally by another individual.	Users assign their own unique password for ISOS to protect their information and to self-manage changes.	Low	High
3.	User's personal information is compromised when transferred through the service provider.	Transmission is encrypted over a secure line (SSEM server). Contractual privacy protection flow downs to service provider. Service provider's security and privacy standards.	Low	High
4.	Inherent risks in providing access to the third party (ISOS)	All ISOS employees are required to abide by contractual obligations including the appended privacy protection	Low	Medium

		schedule and any RRU related privacy policies and guidelines.		

10. Collection Notice

The following collection notice including notification of storage of personal inforamtion is provided prior to the collection of personal information:

The personal information provided is collected under the authority of the *University Act* and is subject to the *Freedom of Information and Protection of Privacy Act*. Your personal information will be used to register you for the International SOS Program (ISOS), an emergency management program supported by Royal Roads University in order to notify you of potential safety events and incidents while travelling or preparing to travel on behalf of Royal Roads University and will also be shared by ISOS with Royal Roads University for reporting purposes. Your personal information will be stored by our third party service provider, International SOS whose servers are located in in Canada (Toronto), USA (Philadelphia, Dallas) and the United Kingdom (London). Your personal information will be stored for up to 3 years depending on the type of information. No other external disclosures will be occurring unless required by law or as directed by you.

By registering with ISOS, you are consenting to the storage of your personal information for this purpose only. Royal Roads University maintains the highest standards for the protection of your personal information that is in our custody and control. As such, Royal Roads University also contractually requires its service providers to equally maintain these standards. If you have any questions please contact Royal Roads University's Privacy Officer at 250 391-2600 Local 4178 or via mail: 2005 Sooke Road, Victoria, BC V9B 5Y2.

Part 3 – Security of Personal Information

11. Please describe the physical security measures related to the initiative.

RRU:

Section 15(1)(l)

Confidentiality agreement for staff accessing personal information in the system.

International SOS is a cloud-based Software-as-a-Service application that an authorised user can access from outside of the RRU physical environment using a variety of devices that may or may not be under RRU control. User accounts and administrative accounts are created on the International SOS platform directly. Thus, any physical security measures that may be implemented at RRU will have no affect on RRU's instance of the International SOS application.

ISOS:

Section 15(1)(l), Section 21

Section 15(1)(l), Section 21

12. **Please describe the technical security measures related to the initiative.**

RRU:
International SOS is a cloud-based Software-as-a-Service application that is not under the control of RRU. Further, user accounts and administrative accounts used by RRU personnel are created on the International SOS application and not anywhere within the RRU environment. Therefore, there are no technical security measures that RRU can take with respect to this application.

ISOS:

Section 15(1)(l), Section 21

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

RRU:
http://policies.royalroads.ca/policies/information-security-policy

ISOS:
ISOS employs a comprehensive suite of information security policies (eg. ISOS Information Security Policy, ISOS Data Protection Policy, Laptop Policy, Clean Desk Policy, etc), see above. International SOS has proved ISO 27001 audit reports and a SOC 2 Type 2 report that confirm these policies are being adhered to.

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.**

RRU:
Access is restricted based on 'a roles and responsibility' basis. Basic users do not have access or the ability to modify other users personal data. Administrators can grant new users basic access by submitting a request to International SOS.

In addition to granting basic user access, Administrators can view and modify travellers profile details and to add trip information on behalf of the traveller. Administrator rights are restricted to two to three individuals. Administrators are required to follow University protocol with regards to user data.

ISOS:

Section 15(1)(l), Section 21

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

RRU:

Administrator rights will be restricted to two to three individuals. This will be determined based on the individuals role at the University. The role must include responsibility for managing those students or staff required to travel internationally as part of University business.

A register of those assigned administrator rights will be maintained by Financial Services. Financial Services will be responsiblie for monitoring admininstrator access and updating the administrator register as roles and responsiilites change.

ISOS:

Section 15(1)(l), Section 21

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?**

Users access the system directly and are responsible for updating personal information as necessary. This allows the traveller to create or modify their personal profile via a secure, password-protected site.

Administrators are also able to view and modify a travellers profile details and add trip information on behalf for the traveller (with their permission). Administrator rights are restricted to two to three individuals. Administrators will be required to follow University protocol with regards to user data.

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

Yes – to provide travel emergency management notifications to employees and students of RRU when necessary.

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.**

All personal information is obtained directly from the traveller profile (also maintained by the traveller) ensuring information is accurate/complete.

19. Administrators also are able to view and modify a travellers profile details and add trip information on behalf for the traveller (with their permission). Administrator rights are restricted to two to three individuals. Administrators are required to follow University protocol with regards to user data. **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?**

Yes, RRU employes a formal Reconds Management schedule that prescribes retention and disposition scheduled for all records. This schedule is currently under review.

Part 5 – Further Information

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

Yes, disclosure of personal information to ISOS occurs when an employee or student travels on behalf of RRU.

Please check this box if the related Information Sharing Agreement (ISA) is attached.	No

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 your privacy office(r).	NA

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.**

Yes.

a. RRU travel management program – emergency notification.
b. Travel services and safety management while on travel status. Personal information includes:
    - First/Last Name
    - Country of Origin
    - Email address
    - Travel Itinerary Information
c. Section 26(c)
d. Obtained, compiled, used and disclosed to facilitate the RRU travel management program.
e. Used by employees/students of RRU in support of the travel management program.

Signatures:

2019-09-09

Don Devenney
Privacy Officer
Royal Roads University

Date

2019-12-09

Jessica Subin
Associate Director, Financial Services
Royal Roads University

Date

2019-09-09

Don Ostergard
Chief Information Officer
Royal Roads University

Date

Approved by:

2019-09-16

Cheryl Eason
Vice-President and CFO
Royal Roads University

Date