Privacy Impact Assessment for:

International SOS

| | | |
|---|---|---|
| Name of Department: | International Education | |
| Program Manager: | Cynthia Murphy, Director, VIU International | |
| Email: | cynthia.murphy@viu.ca | Phone: 236-628-1871 |
| Privacy Officer: | Mike Culbertson, FOI & Privacy Officer | |
| Email | Privacy.officer@viu.ca | Phone: 250-753-3245 ext. 2684 |

# Part 1 – General

## 1. What is the Initiative?

*Describe your initiative in enough detail that a reader who knows nothing about your work will understand the purpose of your initiative and who your partners and other stakeholders are. Describe what you're doing, how it works, who is involved and when or how long your initiative runs.*

- The university is committed to providing students and employees with access to global opportunities and experiences, which enable research, teaching, and learning. These opportunities and experiences are unique and invaluable and include international travel for members of the university community. The university recognizes that where international travel is required, certain risks may exist for travelers and the university. An important component of managing international travel is ensuring that risks to individuals and the institution are managed; reflecting the university's commitment to the health, safety, and security of all members of its community who travel internationally. Engaging a travel risk management provider is an important component of the university's risk management process, and registration with the approved travel registry is required (as outlined section 4.0 of VIU Policy 41.20, International Travel Risk Management). International SOS (ISOS) is a travel registry provider and risk management company that provides international travel medical and security services.

### 1a. Is this initiative a data-linking program under FIPPA?

See Appendix A to determine if your project is a data-linking program.

- No

### 1b. Is this initiative a common or integrated program or activity?

See Appendix B to determine if your project is a common or integrated program or activity.

- No

## 2. What is the scope of the PIA?

*Your initiative might be part of a larger one or might be rolled out in phases. What part of the initiative is covered by this PIA? What is out of scope of this PIA?*

- The ISOS Tracker and traveler assistance are covered in this PIA.

## 3. Are there any related Privacy Impact Assessments?

*Please indicate if this an update on an existing PIA or an additional module that was not covered in the original PIA.*

- There are no previous PIAs for ISOS.

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

*Please list all the elements of information or data that you might collect, use, store, disclose or access as part of your initiative. If your initiative involves large quantities of information or datasets, you can list categories or other groupings of personal information in an appendix.*

- **For Assistance**: Name, Current contact details, Current location, Request for Assistance. Then, depending on the nature of assistance that is being requested, it may also involve the following, only if required, to deliver the service: Date of Birth, Passport Copy, Other Contact Details, Current Address, Home Address, Marital Status, Next-of-Kin, Travel Plans, Employer, Special Category Data (Medical data (frequently), Religion (very rarely), Sexual preference (very rarely))

- **For Tracker:** Data in travel itineraries (Employee/student First Name, Last Name, Airline and Flight Number, Departure and Arrival Cities and Times, Hotel Information including address telephone number, check in and checkout dates, car rental

information, train bookings, pick-up and drop-off dates and locations, email address, mobile telephone number, location, and any additional metadata as instructed by the customer (ex: Employee ID, Business Unit, Division Code, etc.)

### 4a. Did you list personal information in question 4?

*Personal information is any recorded information about an identifiable individual, other than business contact information. Personal information includes information that can be used to identify an individual through association or reference.*

- Yes

- *If yes, go to Part 2*
- *If no, answer* question 5 *and submit questions 1 to 5 to privacy.officer@viu.ca. You do not need to complete the rest of the PIA template.*

## 5. How will you reduce the risk of unintentionally collecting personal information?

*Some initiatives that do not require personal information are at risk of collecting personal information inadvertently, which could result in an information incident.*

- ISOS' products are specifically designed to only collect the data needed to provide a dashboard presentation of users' travel plans/locations; or, in the event of a medical or security emergency, enough information so that the caller can be best assisted when calling into one of our many call Assistance Centers.

## Part 2 – Collection, Use, and Disclosure

*This section will help you identify the legal authority for collecting, using, and disclosing personal information, and confirm that all personal information elements are necessary for the purpose of the initiative.*

### 6. Personal Information Flow Diagram and/or Personal Information Flow Table

*In the table below, list the personal information from question four. Think about how each element of information flows through your project. Your Privacy Officer can help you figure out whether each step is a collection, use, or disclosure, and whether you have the legal authority for the way you're working with the information. Alternatively, you can attach a flow diagram to this PIA.*

| | Describe the way personal information moves through your initiative step by step as if you were explaining it to someone who does not know about your initiative. | Type (Collection, Use or Disclosure) | FIPPA or other legal authority |
|---|---|---|---|
| 1. | **Tracker:** Traveler books travel plan(s) through your authorized Travel Management company; or traveler, themselves, manually enter the itinerary information into the application | Collection | FIPPA 26(c) |
| 2. | Application will display all travel arrangements, per traveler, on a 'dashboard' for the VIU travel administrators to view, track, and locate students/employees in event of crisis. | Use | FIPPA 32(a) |
| 3. | 30 days at the end of the respective trip(s), the data will be removed from the dashboard. The data will then be archived for a set time and eventually deleted based on the ISOS Data Retention, Archiving and Destruction Policy. | | |
| 1. | **For assistance:**<br>caller is traveling and has a medical and security emergency. Calls the | Collection,<br>Use, | FIPPA 26 (C); 32(a) |

| | | | |
|---|---|---|---|
| | local assistance center (AC), as displayed on the mobile app. **Consent to collect data is read/agreed to/recorded by AC staff**. Caller explains the nature of emergency/security issue – AC staff ascertains the situation and provides a resolution to the problem, either by providing the caller with information for them to use, or by contacting one of our 3rd party providers from ISOS network (ambulance service, dentist, doctor, hospital, etc.) to take over the resolution of the emergency.<br>Assistance information is stored in the data centre that is assigned to the location where the assistance is provided.<br>Name, email, passport number/information, personal health information, etc.<br><br>For more details on the information collected, used, disclosed, and retained by ISOS, please read the Members and Patients Privacy Notice. | Disclosure | Privacy notice from ISOS: Callers consent to collect information |

## 7. Risk Mitigation Table

*Thinking through the information flow, identify where there are risks for privacy incidents or information breaches. For each risk, identify a mitigation strategy, as well as the likelihood of an incident, and level of impact on those if their information was breached.*

| Risk | Mitigation Strategy | Likelihood | Impact |
|---|---|---|---|
| Tracker: unauthorized VIU employee gets access to dashboard data on tracker app | • Limit authorization to view travel tracker to designated VIU employees, and only those who are authorized via role-bases access. Principle of "need to know." For list of roles with access, see Q. 19.<br>• Accounts are accessed/protected with username and password and multi-factor authentication. | Low | Medium |
| Tracker: unauthorized ISOS employee accesses Tracker information | • Appropriate internal access controls have been established - privileges and access rights for ISOS employees are role based and granted based on "need-to-know", "need-to-do" and "segregation of duties" to ensure security of traveler personal information.<br>• ISOS employees receive security awareness training<br>• ISOS staff are subject to background verification, criminal records checks, and litigation and insolvency checks where applicable. | Low | Medium |
| Data breach on server where tracker information is stored | • See ISOS security policy for physical, technical, and human resource safeguards and procedures in place to help prevent breaches.<br>• In event of breach, standard breach protocols are covered in contract (section 6), essentially, ISOS will | Low | High |

| | | | | |
|---|---|---|---|---|
| | | notify VIU without undue delay, and will provide VIU with sufficient information to meet notification obligations, and will cooperate in investigation, mitigation, and remediation of each personal data breach. | | |

### 8. Collection or Privacy Notice

*If you are collecting personal information directly from an individual the information is about, FIPPA requires that you provide a collection notice, also known as a privacy notification.*

*A collection notice must contain the following elements:*

- The legal authority and section under FIPPA under which you are collecting personal information.
- The purpose for which you are collecting the personal information and how it will be used.
- The contact information of an employee or officer at VIU who can answer questions about the collection of personal information.

*Contact the privacy office for a collection/privacy notice template.*

- ISOS has their own consent statement that must be agreed to at the time of a call to their Assistance Centers. The caller's agreement to the statement will be recorded and attached to the case file within their case management software.
- For the **Tracker application**, consent to have the information collected and shared is on the booking agent, not ISOS - they are just a receiver of the data from the booking agent.
- For ISOS **mobile app**, consent must be agreed to before the app will function.

## Part 3: Storing Personal Information

### 9. Is any personal information being stored outside of Canada?

*If you're storing personal information outside of Canada, identify the sensitivity of the personal information and where and how it will be stored.*

- Yes

## 9a. Where is the personal information stored?

[redacted]

S. 15(1)(l); S. 21(1)

## 10. Does your initiative involve sensitive personal information?

*Examples of sensitive personal information include personal health information, genetic and biometric data, personal finances, geolocation data, criminal records, counselling records, HR records and payroll records, racial or ethnic origin, sexual orientation, religious, philosophical, or political beliefs, etc.*

- Yes

***If so, will the sensitive personal information collected be stored outside of Canada?***

- Yes

If **yes**, please complete **Part 4**: Assessment for Disclosures Outside of Canada.

If **no**, skip to **Part 5**: Security of Personal Information

## Part 4: Assessment for Disclosures Outside of Canada

*Complete this section if you are disclosing sensitive personal information to be stored outside of Canada. You may need help from your organization's Privacy Officer.*

### 11. Is the sensitive personal information stored by a service provider?

*If yes, fill out the table below, then go to question 13. If no, continue to question 12.*

- Yes

| Information about Service Provider | | |
|---|---|---|
| Name of service provider | Name of cloud infrastructure and/or platform provider(s) (If applicable) | Where is the sensitive personal information stored (including backups)? |
| ISOS Tracker | AWS – private cloud | US |
| ISOS Assistance | See attached contract, [redacted] for cloud data storing locations | Depends on nearest Point of Presence, based on user location. See listed countries in Part3, Q.9a above. For specific data storage locations, see [redacted] |

S. 21(1)

### 12. Provide details on the disclosure, including where and how the personal information is stored.

*Answer this if question 11 does not apply. Be specific about where and how the information is being stored.*

*A collection notice must contain the following elements:*

- The legal authority and section under FIPPA under which you are collecting personal information.

- The purpose for which you are collecting the personal information and how it will be used.
- The contact information of an employee or officer at VIU who can answer questions about the collection of personal information.

*Contact the privacy office for a collection/privacy notice template.*

- Travel information is only visible to the respective traveler, the travel administrator(s) at VIU, and support personnel at ISOS that are in the appropriate positions that require access to client data. For medical/security assistance, this is only available to ISOS employees within our assistance centers.

## 13. Is there a contract that includes privacy-related terms?

*If there is a contract with the provider, please describe any privacy-related terms in the contract.*

- Yes, see attached contract excerpt: [redacted]
  - [redacted] S. 21(1)

## 14. What controls are in place to prevent unauthorized access to sensitive personal information?

*Describe technical, administrative, and/or policy measures in place to protect PI. If using a cloud-based service provider, include a description of controls in each layer of the stack: software level, platform level, infrastructure level.*

- **Clients:** From ISOS' perspective, the only access to any data is through the current application's User Interface. There is no access to the data directly at the server-level for clients.
- **ISOS Employees**: Privileges and Access for ISOS employees is restricted and controlled through "Privilege Access Request Procedure" access to data is based on "need to know", "need-to-do" and "segregation of duties" principles.
- Authorization record of all privileges maintained and annually reviewed.

## 15. How will you track access to sensitive personal information?

*How will you know if sensitive personal information is accessed, including access by service providers? This should include a description of what information is available through logs.*

- [redacted] S. 15(1)(l)
- [redacted] alerts related to access controls are sent to the Security Team when specific actions or events are identified within the logs. S. 21(1)
- [redacted] S. 15(1)(l)

## 16. What are the privacy risks for disclosures outside of Canada?

*Use the table to indicate the privacy risks, potential impacts, likelihood of occurrence and level of privacy risk. For each privacy risk you identify describe a privacy risk response that is proportionate to the level of risk posed.*

| **Privacy risk** | **Impact to individuals** | **Likelihood of unauthorized collection, use, disclosure or storage of the sensitive personal information (low, medium, high)** | **Level of privacy risk (low, medium, high, considering the impact and likelihood)** | **Risk response (This may include contractual mitigations, technical controls, and/or procedural and policy barriers)** | **Is there any outstanding risk? If yes, please describe.** |
|---|---|---|---|---|---|
| Third-party provider mis-handles PI or is in a jurisdiction where privacy laws are not respected. | Foreign governments/authorities or bad actors could use tracker information to locate travelers; or could use sensitive personal | low | medium | According to the ISOS Managers and Clients Privacy Notice: (ISOS) safeguards personal information transferred to third parties by "implementing measures such | |

| | | | | | |
|---|---|---|---|---|---|
| | info – health, Passport info, etc. for identify theft, fraud, extortion, etc. | | | as standard contractual clauses and assessing the third parties that we share your personal information with to minimise the risk to you. Relevant International SOS companies also follow our Binding Corporate Rules which means all our relevant companies meet the same high standards of data protection." | |

## Part 5: Security of Personal Information

*In Part 5, you will share information about the privacy aspect of securing personal information. People, organizations, or governments outside of your initiative should not be able to access the personal information you collect, use, store or disclose. You need to make sure that the personal information is safely secured in both physical and technical environments.*

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

- [redacted] S. 15(1)(l)
- [redacted]
- For more information, please refer to International SOS Information Security Policy V1.3 (updated Jan. 2024).

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

- Layered Cybersecurity Controls: partnered with cybersecurity organizations such as Imperva, CheckPoint, and TrendMicro who enable ISOS with Application, Network, and Host Layer security in prevention mode.
- [redacted]

**Encryption standards:**

- In transit: [redacted]
- At rest: [redacted]

- [redacted] S.21(1)
- [redacted] S. 15(1)(l)

- [redacted]
- [redacted]

S.15(1)(l)

**19. 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.**

**ISOS:**

- [redacted]

[redacted]

- Only authorized employees may have viewing and editing access to the Tracker app in order to track the whereabouts of student/employee travelers so they can provide safety warnings and other pertinent information to travelers.
- VIU users need to verify their identity via email upon creation of account in order to access the portal.
- Authorized VIU employees (or designates*) are designated by nature of their positions:
- [redacted]

S. 15(1)(l)

- International department will set up a database of authorized users and review biannually.

*Authorized employees may appoint designates.

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

- [redacted] S.21(1)

## Part 6: Accuracy/Correction/Retention of Personal Information

*FIPPA section 28 states that a public body must make every reasonable effort to ensure that an individual's personal information is accurate and complete. In this section, you will demonstrate how you intend to keep personal information on file accurate and complete.*

### 21. How is an individual's information updated or corrected?

*FIPPA section 29 states that a person can ask you to correct their personal information in your custody or control. If it is not possible to update or correct (for physical, procedural or other reasons) it must be noted on the record.* ***Please explain how it will be annotated. If personal information will be disclosed to others, how will VIU notify them of the update, correction, or annotation?***

- ISOS has a process where individuals can request access to, correction or deletion of their personal information and an associated dispute resolution process. Registered Travel Tracker users can log into their account to change their personal information or complete the Data Subject Rights Request Form
- Faculty, staff or students can also request that authorized VIU personnel update, correct or delete their personal information.
- The Tracker application is web-based, so any updated information would be visible to both VIU and ISOS designates, as well as the student or employee traveler.

### 22. Does your initiative use personal information to make decisions that directly affect an individual(s)?

FIPPA requires that public bodies keep personal information for a minimum of one year after it is used to make a decision about and individual.

- Yes

### 22a. If you answered "yes" to question 22, please explain the efforts that will be made to ensure that the personal information is accurate and complete.

- Employee personal information is stored [redacted] It is the responsibility of employees to ensure that their personal information is accurate and complete. S. 15(1)(l)
- Student personal information is stored in the [redacted] It is the responsibility of students to ensure that their personal information is accurate and complete. Also, student personal information is collected during activity registration and via orientation processes.

### 23. If you answered "yes" to question 22, do you have an information schedule in place related to personal information used to make a decision?

*FIPPA requires that public bodies keep personal information for a minimum of one year after it is used to make a decision.*

### 24. Do you have a records management schedule in place?

*How long will you keep the personal information collected? Is there a plan in place for retention and deletion? Please also use this question to note how long it will be stored by the service provider (if applicable).*

- The VIU retention and deletion schedule is being developed and is forthcoming [redacted]
- For ISOS, please see attached International SOS Data Retention, Archiving and Destruction Policy. The Retention periods are determined by the category of information (e.g. Medical records and call recordings to assistance centers have different retention periods) as well as legal or contractual obligations or to meet business objectives. For personal data, they must be kept no longer than necessary to protect the rights and freedoms of individual data subjects in accordance with the ISOS data protection policy and data protection regulation.

*Image source: International SOS Data Retention, Archiving and Destruction Policy, Version 2.05, August 2023, p.7.*

## Part 7 – Personal Information Banks

*A personal information bank (PIB) is a collection of personal information searchable by name or unique identifier.*

**25. Will your initiative result in a personal information bank?**

- No

## Part 8 – Further Information

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

- No

**26. Will the information collected be used for research or statistical purposes?**

- No.

## Part 9 - Summary and Proponent Responsibility

*This section is for Privacy Office recommendations as well as any limitations due to privacy concerns.*

- ISOS benchmarks info security and privacy management against the EU General Data Protection Regulation (GDPR) and their data protection policies are generally aligned with the GDPR (see ISOS Data Protection Policy V2.2 , p.4).
- ISOS' information security and privacy policies are well documented – see Part 10 – Resources for links to their various privacy and security documents.
- Using the Travel Tracker mitigates risk to VIU students and employees traveling abroad, as it enhances VIU's ability to help in a medical or security incident.
- ISOS' expertise in handling travel emergencies mitigates risk associated with international travel for VIU students and employees.
- [redacted] S. 13(1)

## Part 10 Resources:

- Members and Patients Privacy Notice. Contains details on information collected, used, disclosed, and retained by ISOS.
- ISOS Processor and Sub-processor list. Contains list and location of processors and sub-processors used to deliver their services. If ISOS receives your personal information and subsequently transfers that information to a third party for processing, they remain responsible for ensuring that such third party processes your personal information to the standard required by the applicable privacy and data protection laws.
- International SOS Data Protection Policy V2.2 (updated Nov. 2023)
- International SOS Information Security Policy V1.3 (updated Jan. 2024)
- Data Retention, Archiving and Destruction Policy V2.05 (updated Aug. 2023)

## Part 11: Signatures

*This PIA accurately documents the data elements and information flow at the time of signing. If there are any changes to the overall initiative, including to the way personal information is collected, used, stored or disclosed, the program area will engage with their Privacy Office and if necessary, complete a PIA update.*

| Role | Name | Electronic signature |
|---|---|---|
| **Initiative lead** | | |
| **Program/Department Manager** (if different from initiative lead) | Cynthia Murphy<br>Director, VIU International | [redacted] S.22(1) |
| **Privacy Officer / Privacy Office Representative** | **Mike Culbertson**<br>FOI & Privacy Officer | |

# Appendix A: Assessments for Data-linking initiatives and Integrated Programs

## Determine whether this program is a "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. If so, you will need to comply with specific requirements under the Act related to data-linking initiatives. | |
| Personal information from one database is linked or combined with personal information from another database; | Y/N |
| The purpose for the linkage is different from those for which the personal information in each database was originally obtained or compiled; | Y/N |
| 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. | Y/N |
| If you have answered "yes" to all three questions, please contact a PCT Privacy Advisor to discuss the requirements of a data-linking initiative. | |

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

# Attachment: ISOS Terms of Service

s. 21(1)

## CERTIFICATE OF SUBSCRIPTION