

Privacy Impact Assessment

PIA# 25-0002

INSTRUCTIONS/INFORMATION:

Why do I need to do a PIA?

Section 69(5.3) of the *Freedom of Information and Protection of Privacy Act* (FOIPPA) requires the head of a public body to conduct a privacy impact assessment (PIA) in accordance with the directions of the minister responsible for FOIPPA.

Do I have to answer all the questions?

Sections marked as “required” must have an answer. Specify *N/A (not applicable)* if appropriate. Other sections not marked mandatory should STILL be answered if the information is known. You will be contacted to answer any questions that are deemed relevant to this assessment so it’s best to be complete.

What if my initiative does not include personal information?

You still need to complete some parts of the PIA to ensure compliance with regulation. Under question “4. Elements of Information or Data”, specify “*no personal information collected*”. Sections that are marked as “*required*” still need to be answered.

What if I have questions?

If you have any questions about FOIPPA generally, you may contact the “*Privacy and Access Officer*” (privacy@tru.ca). For questions specific to this PIA, contact the “*Information Security Director*” (jcuzzola@tru.ca).

Please note: Depending on the dollar amount or length of the agreement you intend to enter into with a third party, you may need to engage the Procurement Services Department. Please see the TRU Purchasing Policy (BRD 02-2) for more information.

Initiative Preamble (Required)

Initiative/ Project/ Program Name:	Migration of Service Desk telephony from Mitel to Solgari for Teams Phones app		
Name of TRU Department/Branch:	IT Client Services		
PIA Drafter (you):	Andrew Skapenko		
Your Email:	askapenko@tru.ca	Phone:	250-214-5117
Service/Vendor:	Solgari		

Privacy Impact Assessment

PIA# 25-0002

Vendor Email:	David Mcallister, VP Technical Operations <david.mcallister@solgari.com>	Phone:	ext. 325 (list of global contact numbers)
---------------	---	--------	---

Have you consulted IT Department for this Initiative/Project/Program?

Yes X No N/A

(If no, it is recommended to consult IT Department first to resolve any potential IT-related issues.)

Part 1 – General

1. Description of the Initiative (required)

Please provide a general description of the initiative and the context in which it functions. This could include the purpose of the initiative, its benefits, the larger process (if any) that it is part of, how it functions, the parties involved, etc. We will be assessing the impacts of this initiative so please include details which help us understand its size/scale and reach.

When TRU student, faculty and/or staff have IT challenges, they call TRU IT Service Desk to access the required support. The Service Desk phones are answered by IT Service Desk Analysts from a physical desk phone. The telephony system is managed through Mitel.

We would like to migrate the calling system from Mitel to Solgari for Teams Phones. The calling will be conducted and managed via Microsoft Teams through [Solgari for Teams Phones app](#).

This initiative will allow the Service Desk to improve the current calling system by:

- Eliminating the need for physical equipment.
- Improving client service by directing incoming calls through Interactive Voice Response (IVR), allowing clients to connect with the relevant area in less time.
- Enhancing client service through features for call quality assessment, monitoring, and reporting.
- Supporting Service Desk Analysts through automatic call transcription and call recording.

There is a Dynamics 365 component of the Solgari app. We will not be using it. The only AI feature that is part of this request is call transcription and call sentiment sensing. As calls come in, they get recorded and transcribed. All phone numbers, call notes and activity will be stored within our Solgari Azure instance.

2. Scope of this PIA (required)

This section should explain exactly what part or phase of the initiative the PIA covers and, where necessary for clarity, what it does not cover.

This PIA request covers the use of the [Solgari app](#), excluding the Dynamics 365 component.

Privacy Impact Assessment

PIA# 25-0002

2-1. Is this initiative recurring in a regular interval, e.g., yearly, or biennially? (required)

The Solgari for Teams Phones will be used on a recurring basis daily.

3. Related Privacy Impact Assessments

None.

4. Elements of Information or Data (required)

Include complete listing of all personal information involved.

- Caller legal name
- TRU ID
- personal email address
- TRU email address
- office location
- address
- date of birth
- emergency contact
- 3rd party contact

Part 2 – Protection of Personal Information

5. Storage or Access outside Canada (required)

Yes. Solgari have a SIP trunk in place with [SIPPIO](#), Solgari representative in Canada. SIPPIO will be the carrier for all inbound/outbound calls, and from there, it all through Solgari's Azure instance. All data will be stored under TRU's tenancy within Solgari's Azure instance. All this is hosted in Microsoft's Azure Central US centre in Iowa.

Please see attached to this PIA a high-level overview of the data flow.

5-1. Is a service provider(s) involved? If so, where is the provider located (e.g. Canada, U.S., or other country)? (required)

The service provider is Solgari. Solgari is located in Ireland. SIPPIO, as Solgari's representative, is also involved by way of having a SIP trunk in Canada for inbound and outbound calls.

Privacy Impact Assessment

PIA# 25-0002

6. Common or Integrated Program or Activity (required)

If you answer yes, please contact the *Privacy and Access Officer*

If you answer “yes” to <u>all</u> 3 of these questions, your initiative qualifies as “a common or integrated program or activity,” and you must comply with requirements under FOIPPA.	
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.	no

7. Data-linking Initiative* (required)

If you answer yes, please contact *Privacy and Access Officer*

If you answer “yes” to all 3 questions, your initiative may be a data linking initiative and you must comply with specific requirements under FOIPPA.	
1. Personal information from one database is linked or combined with personal information from another database;	yes
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

8. Provide a diagram, flowchart, and/or table that shows how your initiative will collect, use, and/or disclose personal information.

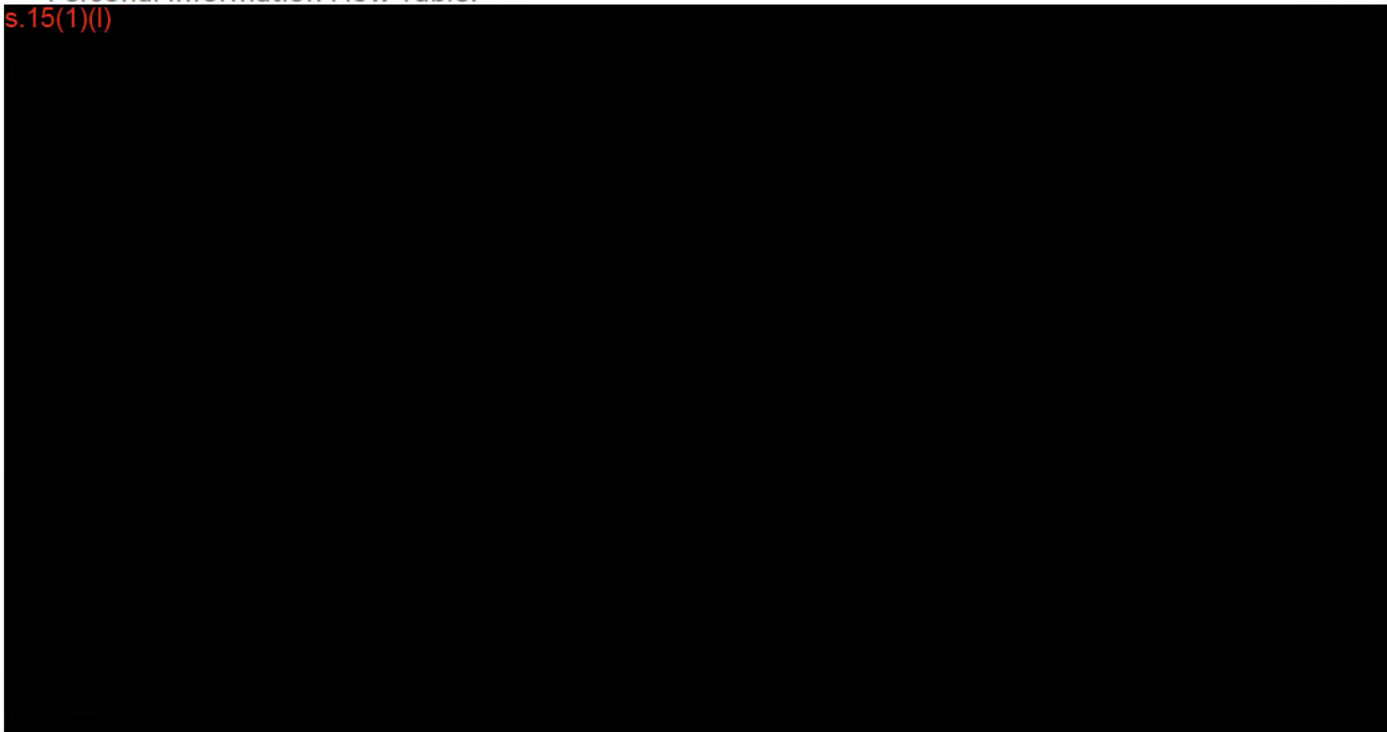
Privacy Impact Assessment

PIA# 25-0002

Your diagram and/or table must also include the authorities for the collection, use, and disclosure of personal information, as laid out in FOIPPA. If the authority comes from other legislation, please identify the applicable act(s) or regulation(s), including specific section references.

Personal Information Flow Table.

s.15(1)(l)



Personal Information Flow Table			
	Description/Purpose	Type	FIPPA Authority
1	Client calls service desk for assistance	Collection	s.26(c)
2	Call will be transcribed via MS Copilot	Collection & Use	s.26(c), s. 32(a)
3	Information will be stored on single tenant for TRU hosted in Azure controlled by Solgari.	Use & Disclosure	s. 32(a), s.33(2)(d)
4	Information available to ITS client services including reports.	Use	s.32(a)

9. Risk Mitigation Table (required)

Privacy Impact Assessment

PIA# 25-0002

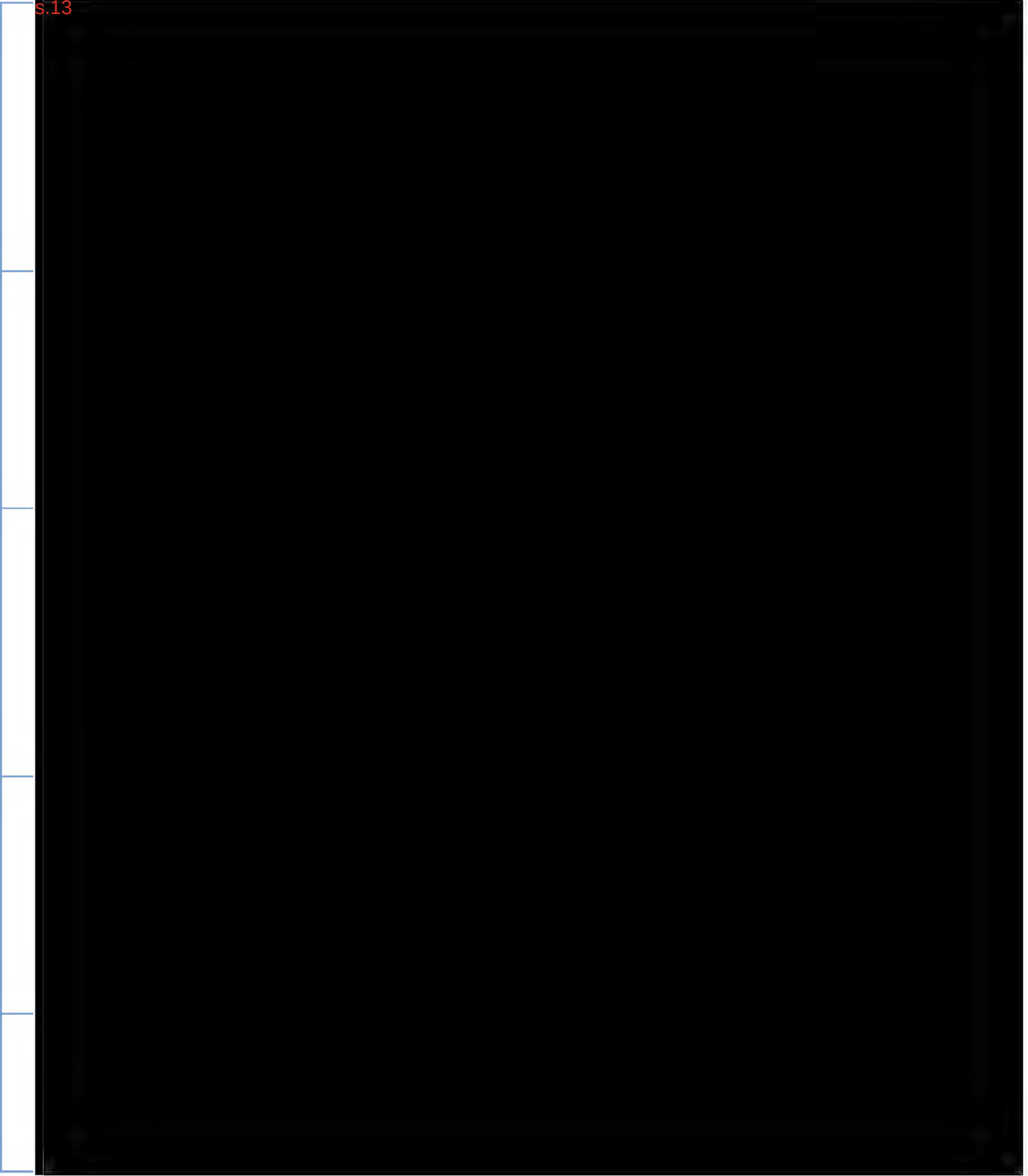
Please identify any privacy risks associated with the initiative and the mitigation strategies that will be implemented. Please identify the likelihood (rare, unlikely, possible, likely, almost certain) and the degree of impact (insignificant, minor, moderate, major, catastrophic).

Risk Mitigation Table					
	Risk	Mitigation Strategy	Likelihood	Impact	Exposure

Privacy Impact Assessment

PIA# 25-0002

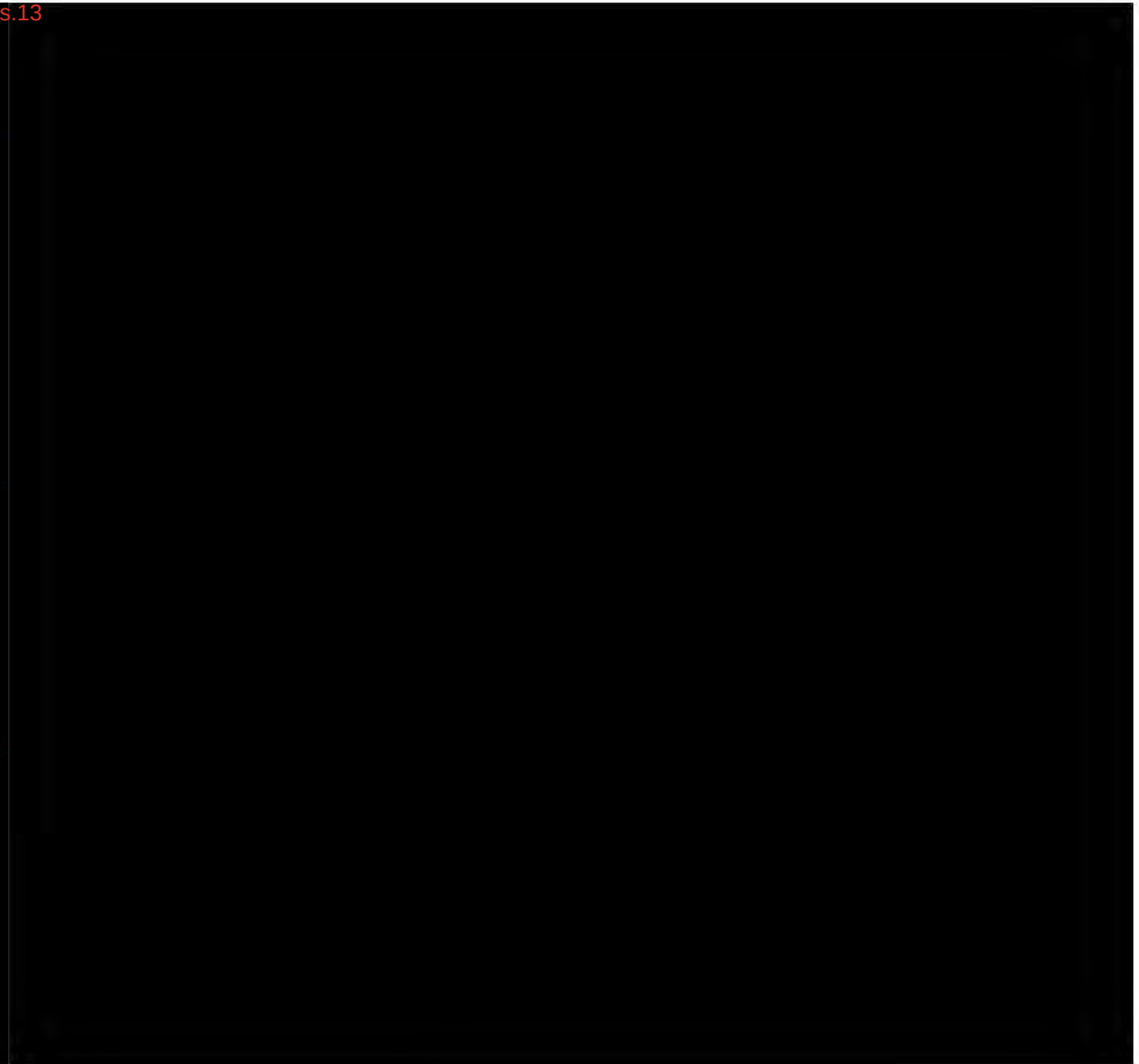
S.13



Privacy Impact Assessment

PIA# 25-0002

s.13



à Exposure rating of *high* or *critical* is of concern. Please contact Director, Information Security to discuss possible solutions.

s.13



Privacy Impact Assessment

PIA# 25-0002

Risk Exposure Matrix

Risk Exposure Matrix		IMPACT				
		Insignificant	Minor	Moderate	Major	Catastrophic
	Almost Certain	Low	Medium	High	Critical	Critical
	Likely	Low	Medium	High	Critical	Critical
	Possible	Insignificant	Low	Medium	High	High
	Unlikely	Insignificant	Low	Low	Medium	Medium
	Rare	Insignificant	Insignificant	Insignificant	Low	Low

10. Collection Notice

If your initiative collects personal information directly from any individuals, you must ensure that all individuals involved are told the following:

1. The purpose for which the information is being collected
2. The legal authority for collecting it, and
3. The title, business address and business telephone number of an officer or employee who can answer questions about the collection.

Please contact *Privacy and Access Officer* for assistance on this.

Standard Collection Notice Statement

This should be presented to participants at or before the time of collection (participation in survey):

“Thompson Rivers University (TRU) collects, uses, discloses and retains personal information in compliance with the BC Freedom of Information and Protection of Privacy Act (FIPPA). Your information is being collected, and used by TRU for the purpose of improving call in service, as authorized by s.26(c) and s.32(a) of FIPPA. This call may be recorded, stored and used for quality assessment and coaching purposes.

For further information about how your personal information is being collected, please contact:

Andrew Skapenko

Manager, IT Client Services

805 TRU Way, Kamloops, BC V2C 0C8

1-250-852-6380

Part 3 – Security of Personal Information

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

All data is stored in Azure cloud. Physical security governed under Microsoft SOC 2 Type 2 compliance.

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

Encryption:

- Data stored in cloud systems is encrypted using AES-256 encryption to ensure data security during storage and backup.

Access Control:

- Access to personal information is limited based on a "least to know" concept with role-based access control systems to ensure only authorized personnel can access sensitive data.

Monitoring and Alerts:

- Various systems, including databases and cloud storage, are monitored regularly. Alerts are set up to identify potential issues.

Backup and Retention:

- Regular backups of critical and sensitive data are maintained (RPO 1 day).
- Off-site backups and archiving strategies are also employed for additional resilience.

Testing and Validation:

- Encryption testing is conducted periodically, with specific systems tested semi-annually or quarterly.

Data Retention Controls:

- Data retention schedules are implemented to ensure data is retained only as long as necessary, aligning with operational, legal, and contractual requirements.

Safeguarding Personal Data:

- Personal data is safeguarded by implementing secure data hosting with best practice measures. However, limitations in preventing unauthorized access are acknowledged. From the Website Privacy Policy:

"Although we take steps to safeguard such information, we cannot be responsible for the acts of those who gain unauthorised access, and we make no warranty, express, implied or otherwise, that we will prevent such access".

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

TRU PAN policy BRD 16-1 as well as internal Information Security policies. In addition Solgari policies:

Data Protection Policy:

- Outlines compliance with the GDPR and other relevant legislation, ensuring lawful, fair, and secure processing of personal data.
- Specifies the principles of data protection, including accountability, data minimization, storage limitation, and security of personal data against unauthorized access or accidental loss.

Data Retention and Destruction Policy:

- Provides guidelines for retaining and securely disposing of records after the specified retention period.
- Emphasizes appropriate destruction methods for both physical and digital records (e.g., shredding paper, securely deleting digital files).

Privacy Notice Procedure:

- Ensures compliance with GDPR requirements regarding informing data subjects about the use of their data, safeguarding their rights, and implementing privacy-by-design principles.

Data Subject Request Procedure:

- Details the steps to handle data subject requests, including verifying identity, assessing validity, and ensuring timely responses to protect the data subject's rights.

Technical Safeguards:

- The use of encryption (e.g., AES-256) to protect sensitive data during storage and transmission

Monitoring and Testing Procedures:

- Regular monitoring, testing, and validation of systems to identify potential vulnerabilities and ensure compliance with security measures.

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. (required)

The data will reside within TRU's tenant on Solgari's Azure. Only users with approved roles will have access to the data. Specifics include:

Role-Based Access Control (RBAC):

- *Access to personal information is governed by a "least to know" principle, meaning only personnel with a legitimate need to access certain information for their role are authorized to do so. This ensures that personal data is not unnecessarily exposed.*

Authorization Levels:

- *Employees and service providers are required to follow Solgari's information classification standard, ensuring that access to confidential records is restricted to authorized individuals only.*

Data Integrity Measures:

- *Measures are implemented to maintain data integrity, including processes and policies to ensure that personal information is accurate, complete, and protected from unauthorized changes. Requests for changes to personal information require proper verification to prevent errors or unauthorized actions.*

Audit and Monitoring:

- *Regular monitoring and alerts are in place to detect unauthorized changes or access attempts in systems where personal data is stored. For example, quarterly monitoring is conducted for systems storing customer and employee data.*

Change Request Validation:

- *Data subject requests, such as corrections or deletions, undergo evaluation to confirm validity and authorization before any changes are applied. For instance, identity verification is mandatory before fulfilling any request to ensure only legitimate changes are processed.*

System Encryption:

- *Data stored in cloud systems is encrypted using AES-256 encryption, providing an additional layer of protection against unauthorized access or manipulation of personal information.*

Employee Training:

- *Staff involved in handling personal data are trained in good data protection practices, reducing the likelihood of unauthorized or accidental changes.*

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

The personal information is accessed by users with assigned licenses and approved access roles. A list of users with access to the app can be accessed through Admin Hub on Solgari's portal. In addition:

Access Monitoring and Logging:

- Systems storing personal data (e.g., databases, cloud storage) are regularly monitored, and alerts are set up to detect unauthorized access or changes.
- Periodic reviews, such as quarterly monitoring of sensitive systems, are conducted to ensure compliance with access control policies.

Role-Based Access Control (RBAC):

- Access is assigned based on specific roles, and access permissions are granted only to authorized personnel who need access for their tasks. These permissions are centrally managed and reviewed periodically.

Data Subject Request Logs:

- Requests for access to, modification of, or erasure of personal data are logged in the **Data Subject Request Register**, which tracks details such as:
 - Name and identity of the requester.
 - Type of request (e.g., access, rectification).
 - Personal data involved.
 - Actions taken and the responsible personnel.

Verification of Access Requests:

- All access or changes to personal data are contingent upon identity verification of the individual making the request. This step ensures that unauthorized individuals cannot access or modify personal information.

Encryption and Backup Systems:

- Data stored in encrypted systems includes auditing capabilities to log access events and ensure visibility into who accessed the data, when, and for what purpose.

Periodic Testing:

- Regular validation of monitoring systems and access logs is conducted semi-annually or quarterly to maintain the integrity of access controls.

Part 4 – Accuracy/Correction/Retention of Personal Information

- 16. How is an individual's personal information updated or corrected? If it is not updated or corrected (for physical, procedural or other reasons) please explain how it will be annotated.**

An individual's information, as taken and transcribed by Microsoft Copilot during the call, is verified against an individual's account in Banner during the call. After that, the call notes are entered to TeamDynamix where the individual's information resides. Should the ticket data require updating, it can be done by editing the ticket notes.

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

No. An individual's personal information is only used to verify an individual's identity before providing requested IT support.

- 18. If you answered "yes" to question 17, please explain the efforts that will be made to ensure that the personal information is accurate, complete and up-to-date.**

For example: check to see that the information was obtained from a reputable source such as another government agency.

Not applicable.

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

Privacy Impact Assessment

PIA# 25-0002

If you do not yet have a schedule, please document how these records will be kept until the schedule is in place. Please contact Manager, Information Services.

Not applicable

Part 5 – Further Information

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

For example: your initiative involves a regular exchange of personal information (both collection and disclosure) with other government(s) and/or other agencies in order to provide services to your clients.

No data disclosure.

Please check this box if the related Information Sharing Agreement (ISA) is attached. If you require assistance completing an ISA, please contact Legal Services.

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

For example: your initiative involves disclosing information to PhD students so that they can conduct research.

No.

Please check this box if the related Research Agreement (RA) is attached. If you require assistance completing an RA, please contact Privacy and Access Officer.

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.

A personal information bank means a collection of personal information that is organized or retrievable by the name of an individual or by an identifying number, symbol, or other particular assigned to an individual.

Yes. 69(6): The head of a public body that is not a ministry must make available for inspection and copying by the public a directory that lists the public body's personal information banks and includes the following information with respect to each personal information bank:

(a) its title and location;

- *Solgari for Teams Phone App. Hosted within Solgari Azure Cloud*

(b) *a description of the kind of personal information and the categories of individuals whose personal information is included;*

- *see part 1. Question 4*

(c) *the authority for collecting the personal information;*

- *s. 26(c) "the information relates directly to and is necessary for a program or activity of the public body,"*

(d) *the purposes for which the personal information was obtained or compiled and the purposes for which it is used or disclosed;*

- *To allow the ITS Service Desk to improve the calling system*

(e) *the categories of persons who use the personal information or to whom it is disclosed;*

- *For ITS Service Desk use*

(f) *information required under subsection (7).*

- *N/A*

Part 6 – Canada’s Anti-Spam Legislation (CASL) Compliance

23. Please confirm if you plan on emailing, texting, or instant messaging as part of your project. (required)

No. The individuals calling IT Service Desk will receive ticket-related communication through TeamDynamix, not Solgari.

24. If you answered yes to question 23, please explain the purpose(s) of the messages you intend to send. Be sure to note any messages involving promotional activities, including links to the TRU public website or other Internet site(s). The purpose(s) you provide will help us identify whether the overall communication is a commercial electronic message (CEM¹)?

Not applicable.

25. If your communication message does fall under CEM rules, you must comply with the unsubscribe mechanism and identification requirements under CASL. Please confirm your

¹ If your initiative or program sends commercial electronic messages (CEMs), such as emails promoting a product or service, you must comply with CASL's requirements to: (1) obtain consent, (2) provide identification information, and (3) include an unsubscribe mechanism in each message. Please note that an electronic message that contains a request for express consent is also considered to be a CEM under CASL.

Privacy Impact Assessment

PIA# 25-0002

method of unsubscribe mechanism that must be processed within 10 business days and how you will meet the identification requirements?

Not applicable.

26. If you do meet the definition of CEM, please confirm that you have a records retention schedule that will ensure that consent communications, both paper and electronic, are stored appropriately and retained for three years after the last communication?

Not applicable.

Part 7 – Common Vulnerabilities and Exposures (CVE) Assessment

(This section to be completed by the **Information Security Office**). If your initiative involves the transmission of personal data between TRU and the vendor, or from the vendor to 3rd parties, then TRU may ask for the name of the software used to determine if there are applicable CVEs.

No CVEs found

Privacy Impact Assessment

PIA# 25-0002

Part 8a – Information Security Director Comments

Please ensure that the collection notice (question 10) be played to the student/staff/faulty upon phoning and prior to the collection of any information. I have no further concerns.

John Cuzzola	s.22	2025-0-31
Information Security Director	Signature	Date

Part 8b – Privacy Officer Comments

Privacy and Access Officer	Signature	Date
----------------------------	-----------	------

Privacy Impact Assessment

PIA# 25-0002

Part 9 – Program Area Signatures

Program/Department Manager	Signature	Date
John Cuzzola		
Information Security Director	Si	Date
Senior Manager, Program Area/Division	Signature	Date
General Manager	Signature	Date
General Manager	Signature	Date

A Final Copy of this PIA (with all signatures) shall be kept on record by the program area responsible for this project. The signed original record will be retained by the FOI and Privacy Office. *If you have any questions about FOIPPA generally, you may contact the “Privacy and Access Officer” (privacy@tru.ca). For questions specific to this PIA, contact the “Information Security Director” (jcuzzola@tru.ca).*