PIA02309 — Wellspring Sophia

PIA REVIEW – EXECUTIVE REPORT



PREFACE

This document forms part of UBC Safety and Risk Services (SRS) PrISM's internal documentation for support and administration of the Privacy Impact Assessment (PIA) Review Process. In particular, it documents the final report of the specified PIA review.

This segment serves to provide and record document control capabilities for this document.

Controlled Document

The template and final report documents are controlled documents. The master electronic versions of each reside on the SRS TeamShare S-drive. Any copies or versions not provided directly by the SRS PrISM team, or which have a broken chain of custody, are not to be considered as official copies.

Document Control

The following sub-sections provide a record of the base document template revision history and control.

CONTRIBUTORS

CONTRIBUTOR	DEPARTMENT	POSITION
Taylor Bohn	Safety and Risk Services	Privacy and Information Security Risk Advisor

Figure 1 - Major Document Revision Approval History

TEMPLATE REVISION HISTORY

REVISION #	DATE	REVISED BY	DESCRIPTION
1.0	2023-06-23	Taylor Bohn	Report Creation

Figure 2 - Document Revision History and Revision Summary

TEMPLATE REVISION APPROVAL

REVISION #	DATE	REVISED BY	DESCRIPTION
1.00	2023-06-23	William Sharp	Initial release of document

Figure 3 - Major Document Revision Approval History



TABLE OF CONTENTS

PREFACE		1
Contro	olled Document	1
Docum	nent Control	1
CON	ITRIBUTORS	1
TEM	IPLATE REVISION HISTORY	1
TEM	IPLATE REVISION APPROVAL	1
TABLE OF	CONTENTS	2
TABLE OF	FIGURES	4
PART 1:	GENERAL INFORMATION & OVERVIEW	5
1.1	Executive Summary	5
1.2	Description of the Program, System, Application, or Initiative Assessed	5
1.3	Scope	5
1.4	Data Elements	5
1.5	Storage or Access Outside of Canada (including back-ups and recovery)	6
1.6	Data-Linking Initiative	6
1.7	Is this a Common or Integrated Program or Activity?	6
PART 2:	PROTECTION OF PERSONAL INFORMATION	6
2.1	Personal Information Flow Diagram / Table	6
2.2	Risk Mitigation Table	7
2.3	Collection Notice	8
2.4	Consent for Storage/Access Outside of Canada & Opt-Out Procedure (If Any)	8
2.5	Consent Withheld Procedure	8
PART 3:	SECURITY OF PERSONAL INFORMATION	8
3.1	Physical Security Measures	8
3.2	Technical Security Measures	8
3.3	Security Policies, Procedures, and Standards	8
3.4	Tracking Access / Access Controls	8
PART 4:	ACCURACY, CORRECTION, AND RETENTION	9
4.1	Updating and Correcting Personal Information	9
4.2	Decisions That Directly Affect an Individual	9
4.3	Records Retention and Disposal	9



PART 5:	FURTHER INFORMATION	9
5.1	Systematic Disclosures of Personal Information	
5.2	Access for Research or Statistical Purposes	9
5.3	Other Applicable Legislation and Regulations	9
PART 6:	ACCESS AND PRIVACY MANAGER COMMENTS	10
6.1	Information or Materials Reviewed	10
6.2	Analysis and Findings	10
6.3	Conditions of Approval	10
6.4	Review and Distribution	11



TABLE OF FIGURES

Figure 1 - Major Document Revision Approval History	i
Figure 2 - Document Revision History and Revision Summary	
Figure 3 - Major Document Revision Approval History	
, , , , , , , , , , , , , , , , , , , ,	
Figure 4 - Risk Mitigation Table	,



PART 1: GENERAL INFORMATION & OVERVIEW

1.1 Executive Summary

The UBC University-Industry Liaison Office (UILO) is responsible for managing contracts, relationships and patents associated with UBC. UILO will be moving the existing repository to a new service, the Sophia Knowledge Management System, by Wellspring. Sophia is a cloud-based knowledge management application designed for small to large laboratories and facilities, enabling streamlining of the knowledge supply chain lifecycle, including capturing information on assets, inventions, and patents, as well as managing contracts as well as agreements.

1.2 Description of the Program, System, Application, or Initiative Assessed

The University-Industry Liaison Office (UILO) manages over 3000 contracts and agreements per year with a total value to the University of more than \$200 million. To effectively manage these contracts and associated intellectual property (IP) assets on behalf of the university the UILO requires a sophisticated database capable of managing both IP/technology and agreements/contracts. We have selected the Wellspring Sophia software to replace our current system.

RISK CLASSIFICATION

The inherent privacy risk classification level of this PIA submission is **4** - **High**. The residual risk classification level of this PIA submission at closure is **3** - **Low**.

1.3 Scope

Collection of personal information by authorized UBC administrators using Wellspring application, as outlined in this PIA.

1.4 Data Elements

The system will capture the names and contact details (addresses, personal phone numbers) of researchers (both Faculty and Students) at UBC who have submitted invention disclosures. In many cases citizenship data will also be captured (necessary for patent applications). It will further capture information about payments made to those researchers.

Personal information is captured primarily for the following reasons (a) to confirm the identify of inventors on patents, (b) to ensure that we can distribute revenue to inventors per UBC Policy LR11, and (c) to provide required information to national patent offices.

Researchers are required to provide their names and contact details (i) when completing invention disclosures, and (ii) when completing revenue sharing agreements.

UBC Finance (accounts payable) will give PI to researchers to process revenue sharing benefits. National Patent Offices require certain researchers PI (names, home addresses, citizenship) to file patents in UBC's name.



1.5 Storage or Access Outside of Canada (including back-ups and recovery)

Personal information will be securely stored on AWS servers within Canada, with backup on Google Cloud Platform, as outlined in the diagram below.

1.6 Data-Linking Initiative

This project is not considered a data linking initiative as contemplated under s.(36) of FIPPA.

1.7 Is this a Common or Integrated Program or Activity?

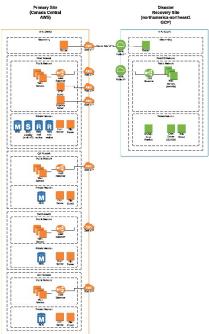
This project is not considered a common or integrated program or activity as defined in Schedule 1 of FIPPA.

PART 2: PROTECTION OF PERSONAL INFORMATION

2.1 Personal Information Flow Diagram / Table

Users will log-in to the Sophia system via Single Sign-On using UBC CWL. Wellspring will integrate with UBC's SSO/SAML system to ensure user authentication.

The following data flow diagram has been provided in support of this PIA, outlining the data storage and backup locations:



The following list of sub-processors has been identified:

- AWS Cloud Hosting Service Central Canada AWS (Primary) and Montreal (DR).
- Zendesk Help Center / Sub-processor of certain end-user data (name, email).
- Google Gmail Internal email Communication Tool / May contain end-user names and emails.
- Basecamp Project Collaboration Software / May contain end-user names and emails.
- Sisense Business Intelligence Tool / May be used to support dashboards with names.

The vendor has confirmed no personal information is shared with third parties by Wellspring.



2.2 Risk Mitigation Table

The following table indicates the associated risk levels as applicable and the potential or intended mitigation steps.

Category: Security							
Risk	Ref#	Inherent Likelihood	Inherent Impact	Response	Residual Risk		
Retaining PI longer	RK0021438	4 - High	3 - Significant	Mitigate	3 - Medium		
than necessary	Mitigation Plan:						
	A data retention plan has not been submitted by the project. The unit is recommended to work with						
		lanagement to develop d			given the sensitivity of		
	the data eleme	nts and research data to	be collected within th	e service.			
Inadequate third party	RK0021446	4 – High	4 – Major	Mitigate	3 - Medium		
information sharing	Mitigation Plan		'		<u>'</u>		
controls	No personal inf	ormation is shared with	third parties by Wellsp	oring. There is some	required information		
	sharing within I	UBC between units, inclu	ding financial and reve	enue sharing agreer	ments, citizenship, and		
	taxation inform	ation. This is required fo	r regulatory and comp	liance purposes.			
Disposing of personal	RK0021572	4 - High	4 - Major	Mitigate	3 - Medium		
information using	Mitigation Plan		4 - Iviajoi	wiitigate	3 - Medidili		
inadequate methods	_	 ecommended to develop	a detailed disposal pl	an, outlining how d	ata will be migrated		
		system and what will ha	• • •	_	_		
- "		·	T	<u> </u>	<u> </u>		
Over-collection of	RK0021125	4 – High	4 - Major	Mitigate	3 - Medium		
personal information	Mitigation Plan		- d f th		.:		
		nation collected is requir innovation/patent holde	• •		•		
	required personal information, as outlined within the Data Elements section, and to avoid collecting SIN number or financial information (deemed Very High Risk, per Security Classification of UBC						
				per Security Classifi	cation of UBC		
	SIN number or		emed Very High Risk,				
	SIN number or Electronic Infor	financial information (de	emed Very High Risk, curity Standard U1). T	his data should be	obtained from other		
	SIN number or Electronic Infor	financial information (de mation Information Se	emed Very High Risk, curity Standard U1). T	his data should be	obtained from other		
	SIN number or Electronic Infor UBC databases The project has	financial information (de mation Information Se which should remain the agreed to limit collectio	emed Very High Risk, curity Standard U1). T e sole repository of suc n to the data required	his data should be on the information, such and to avoid collections.	obtained from other n as Workday.		
	SIN number or Electronic Infor UBC databases The project has Sophia. This wil	financial information (de mation Information Se which should remain the agreed to limit collectio Il be collected and retain	emed Very High Risk, curity Standard U1). To sole repository of such to the data required ed locally on an encry	his data should be on the information, such and to avoid collections of the spreadsheet, a	obtained from other n as Workday. Cting SIN within s this data is required		
	SIN number or Electronic Infor UBC databases The project has Sophia. This wil as part of the ir	financial information (de mation Information Se which should remain the agreed to limit collectio Il be collected and retain evention disclosure and f	emed Very High Risk, curity Standard U1). To sole repository of such to the data required ed locally on an encry or UBC Accounts Paya	his data should be on the control of	obtained from other n as Workday. cting SIN within s this data is required ing revenue and		
	SIN number or Electronic Infor UBC databases The project has Sophia. This wil as part of the ir correct tax slips	financial information (de mation Information Se which should remain the agreed to limit collection to be collected and retain evention disclosure and for are created. Other pers	emed Very High Risk, curity Standard U1). To sole repository of such to the data required ed locally on an encry or UBC Accounts Paya	his data should be on the control of	obtained from other n as Workday. cting SIN within s this data is required ing revenue and		
	SIN number or Electronic Infor UBC databases The project has Sophia. This wil as part of the ir	financial information (de mation Information Se which should remain the agreed to limit collection to be collected and retain evention disclosure and for are created. Other pers	emed Very High Risk, curity Standard U1). To sole repository of such to the data required ed locally on an encry or UBC Accounts Paya	his data should be on the control of	obtained from other n as Workday. cting SIN within s this data is required ing revenue and		
Category: Security	SIN number or Electronic Infor UBC databases The project has Sophia. This will as part of the ir correct tax slips invention disclose.	financial information (de mation Information Se which should remain the agreed to limit collectio Il be collected and retain evention disclosure and f are created. Other pers osure process.	emed Very High Risk, curity Standard U1). To sole repository of such to the data required ed locally on an encry or UBC Accounts Paya onal information data	his data should be on the information, such and to avoid collect of the street of the the street of	obtained from other nas Workday. cting SIN within s this data is required ing revenue and red as part of the		
Risk	SIN number or Electronic Infor UBC databases The project has Sophia. This will as part of the ir correct tax slips invention disclose.	financial information (de mation Information Se which should remain the agreed to limit collectio II be collected and retain evention disclosure and for are created. Other persosure process. Inherent Likelihood	emed Very High Risk, curity Standard U1). To sole repository of such to the data required ed locally on an encry, or UBC Accounts Paya onal information data	his data should be on the information, such and to avoid collected spreadsheet, a ble to ensure licens elements are requi	obtained from other n as Workday. cting SIN within s this data is required ing revenue and red as part of the Residual Risk		
Risk Weak or absence of	SIN number or Electronic Infor UBC databases The project has Sophia. This will as part of the ir correct tax slips invention disclose.	financial information (de mation Information Se which should remain the agreed to limit collectio Il be collected and retain evention disclosure and f are created. Other pers osure process.	emed Very High Risk, curity Standard U1). To sole repository of such to the data required ed locally on an encry or UBC Accounts Paya onal information data	his data should be on the information, such and to avoid collect of the street of the the street of	obtained from other nas Workday. cting SIN within s this data is required ing revenue and red as part of the		
Risk Weak or absence of technical security	SIN number or Electronic Infor UBC databases The project has Sophia. This will as part of the ir correct tax slips invention disclose. Ref# RK0021574	financial information (de mation Information Se which should remain the agreed to limit collection be collected and retain evention disclosure and for are created. Other persosure process. Inherent Likelihood 4 – High	emed Very High Risk, curity Standard U1). To sole repository of such to the data required ed locally on an encry, or UBC Accounts Paya onal information data	his data should be on the information, such and to avoid collected spreadsheet, a ble to ensure licens elements are requi	obtained from other n as Workday. cting SIN within s this data is required ing revenue and red as part of the Residual Risk		
Risk Weak or absence of	SIN number or Electronic Infor UBC databases The project has Sophia. This will as part of the ir correct tax slips invention disclose. Ref# RK0021574 Mitigation Plan	financial information (de mation Information Se which should remain the agreed to limit collection be collected and retain evention disclosure and for are created. Other persosure process. Inherent Likelihood 4 - High	emed Very High Risk, curity Standard U1). To sole repository of such to the data required ed locally on an encry or UBC Accounts Paya onal information data Inherent Impact 4 - Major	his data should be on information, such the information, such and to avoid collected spreadsheet, able to ensure licenselements are required. Response Mitigate	obtained from other in as Workday. cting SIN within is this data is required ing revenue and red as part of the Residual Risk 3 - Medium		
Risk Weak or absence of technical security	SIN number or Electronic Infor UBC databases The project has Sophia. This wil as part of the ir correct tax slips invention disclo Ref# RK0021574 Mitigation Plar The vendor has	financial information (de mation Information Se which should remain the sagreed to limit collection in the collected and retain evention disclosure and for are created. Other personance of the collected in t	emed Very High Risk, icurity Standard U1). Te sole repository of such to the data required ed locally on an encry or UBC Accounts Paya onal information data Inherent Impact 4 - Major	his data should be on the information, such the information, such and to avoid collected spreadsheet, able to ensure licenselements are required. Response Mitigate Mitig	obtained from other in as Workday. Citing SIN within is this data is required ing revenue and red as part of the Residual Risk 3 - Medium		
Risk Weak or absence of technical security	SIN number or Electronic Infor UBC databases The project has Sophia. This wil as part of the ir correct tax slips invention disclo Ref# RK0021574 Mitigation Plar The vendor has completed HEC	financial information (de mation Information Se which should remain the sagreed to limit collection in the collected and retain mention disclosure and feare created. Other personare process. Inherent Likelihood 4 – High I: provided security attest VAT. These documents of	emed Very High Risk, icurity Standard U1). To sole repository of such to the data required ed locally on an encry or UBC Accounts Paya onal information data Inherent Impact 4 - Major ations in the form of leading to the form of leading to the form of leading to the form of t	his data should be on the information, such and to avoid collected spreadsheet, a ble to ensure licenselements are required. Response Mitigate CO 27001 certification are in place to mission to mission the collection of the col	cting SIN within s this data is required ing revenue and red as part of the Residual Risk 3 - Medium on as well as a tigate privacy and		
Risk Weak or absence of technical security	SIN number or Electronic Infor UBC databases The project has Sophia. This wil as part of the ir correct tax slips invention disclose. Ref# RK0021574 Mitigation Plar The vendor has completed HEC security risks. T	financial information (de mation Information Se which should remain the agreed to limit collection in the collected and retain mention disclosure and for are created. Other personare process. Inherent Likelihood 4 – High It provided security attest VAT. These documents of the information containe	emed Very High Risk, icurity Standard U1). To sole repository of such to the data required ed locally on an encry or UBC Accounts Paya onal information data Inherent Impact 4 - Major ations in the form of leading to the HECVAT sugged in the HECVAT sugged.	his data should be on the information, such and to avoid collected spreadsheet, a ble to ensure licenselements are required. Response Mitigate CO 27001 certification are in place to miests that the vendor	cting SIN within s this data is required ing revenue and red as part of the Residual Risk 3 - Medium Ion as well as a tigate privacy and is heavily reliant on		
Risk Weak or absence of technical security	SIN number or Electronic Infor UBC databases The project has Sophia. This wil as part of the ir correct tax slips invention disclosed Ref# RK0021574 Mitigation Plar The vendor has completed HEC security risks. T the AWS hostin	financial information (de mation Information Se which should remain the agreed to limit collection in the collected and retain mention disclosure and for are created. Other personare process. Inherent Likelihood 4 – High It provided security attest VAT. These documents of the information containing platform for security of	emed Very High Risk, icurity Standard U1). To sole repository of such to the data required ed locally on an encry or UBC Accounts Paya onal information data Inherent Impact 4 - Major ations in the form of leading to the HECVAT suggeontrols. However, the	his data should be on the information, such and to avoid collected spreadsheet, a ble to ensure licenselements are required. Response Mitigate CO 27001 certification are in place to misst that the vendor vendor's own docu	cting SIN within s this data is required ing revenue and red as part of the Residual Risk 3 - Medium Ion as well as a tigate privacy and is heavily reliant on mentation and		
Risk Weak or absence of technical security	SIN number or Electronic Infor UBC databases The project has Sophia. This wil as part of the ir correct tax slips invention disclosed Ref# RK0021574 Mitigation Plar The vendor has completed HEC security risks. T the AWS hostin internal process.	financial information (de mation Information Se which should remain the agreed to limit collection in the collected and retain mention disclosure and for are created. Other personare process. Inherent Likelihood 4 – High It provided security attest VAT. These documents of the information containe	emed Very High Risk, curity Standard U1). To sole repository of such that is a sole repository of UBC Accounts Paya onal information data info	his data should be on the information, such and to avoid collected spreadsheet, a ble to ensure licenselements are required. Response Mitigate CO 27001 certification are in place to miss that the vendor vendor's own docuionally recognized for the information and the information are in placed to miss that the vendor vendor's own docuionally recognized for the information and the information are in placed to miss that the vendor vendor's own docuionally recognized for the information and the information are in placed to the information are information.	cting SIN within s this data is required ing revenue and red as part of the Residual Risk 3 - Medium Ion as well as a tigate privacy and is heavily reliant on mentation and rameworks and		
Risk Weak or absence of technical security	SIN number or Electronic Infor UBC databases The project has Sophia. This wil as part of the ir correct tax slips invention disclosed Ref# RK0021574 Mitigation Plar The vendor has completed HEC security risks. T the AWS hostin internal process.	financial information (de mation Information Se which should remain the sagreed to limit collection in the collected and retain mention disclosure and for are created. Other personare process. Inherent Likelihood 4 – High It provided security attest VAT. These documents of the information containents grapher for security coses suggest that they strictly. ISO, NIST). Per the HECV	emed Very High Risk, curity Standard U1). To sole repository of such that is a sole repository of UBC Accounts Paya onal information data info	his data should be on the information, such and to avoid collected spreadsheet, a ble to ensure licenselements are required. Response Mitigate CO 27001 certification are in place to miss that the vendor vendor's own docuionally recognized for the information and the information are in placed to miss that the vendor vendor's own docuionally recognized for the information and the information are in placed to miss that the vendor vendor's own docuionally recognized for the information and the information are in placed to the information are information.	cting SIN within s this data is required ing revenue and red as part of the Residual Risk 3 - Medium Ion as well as a tigate privacy and is heavily reliant on mentation and rameworks and		
Risk Weak or absence of technical security controls	SIN number or Electronic Infor UBC databases The project has Sophia. This wil as part of the ir correct tax slips invention disclosed and the correct tax slips invention disclosed and tax slips invention and	financial information (de mation Information Se which should remain the sagreed to limit collection in the sagreed to	emed Very High Risk, curity Standard U1). To sole repository of such that is sole repository or UBC Accounts Paya onal information data Inherent Impact 4 - Major Inherent Impact 4 - Major ations in the form of light of the HECVAT suggestion of the HECVAT, the controls that is sole to the HECVAT and the HECVAT suggestion of	his data should be on the information, such the information of the information, such the information of the informati	cting SIN within s this data is required ing revenue and red as part of the Residual Risk 3 - Medium Ion as well as a tigate privacy and is heavily reliant on mentation and rameworks and been put in place are		
Risk Weak or absence of technical security controls Use of third-party	SIN number or Electronic Infor UBC databases The project has Sophia. This wil as part of the ir correct tax slips invention disclosed and the second of the intervention disclosed and the second of the security risks. The vendor has completed HEC security risks. The AWS hostin internal procession standards (e.g., acceptable for the second of the seco	financial information (de mation Information Se which should remain the sagreed to limit collection in the sagreed to the s	emed Very High Risk, curity Standard U1). To sole repository of such that is a sole repository of UBC Accounts Paya onal information data info	his data should be on the information, such and to avoid collected spreadsheet, a ble to ensure licenselements are required. Response Mitigate CO 27001 certification are in place to miss that the vendor vendor's own docuionally recognized for the information and the information are in placed to miss that the vendor vendor's own docuionally recognized for the information and the information are in placed to miss that the vendor vendor's own docuionally recognized for the information and the information are in placed to the information are information.	cting SIN within s this data is required ing revenue and red as part of the Residual Risk 3 - Medium Ion as well as a tigate privacy and is heavily reliant on mentation and rameworks and		
Risk Weak or absence of technical security controls Use of third-party applications with	SIN number or Electronic Infor UBC databases The project has Sophia. This wil as part of the ir correct tax slips invention disclosed. Ref# RK0021574 Mitigation Plar The vendor has completed HEC security risks. T the AWS hostin internal process standards (e.g., acceptable for its RK0021439 Mitigation Plar	financial information (de mation Information Se which should remain the sagreed to limit collection in the sagreed to the s	emed Very High Risk, curity Standard U1). To sole repository of such that is sole repository of UBC Accounts Paya onal information data Inherent Impact 4 - Major Inherent Impact 4 - Major ations in the form of light of the HECVAT suggestion of the HECVAT suggestion of the HECVAT suggestion of the HECVAT, the controls that is sole and the HECVAT, the controls that is sole and the HECVAT, the controls that is sole and the HECVAT of the sole and the sole and the HECVAT of the sole and the s	his data should be on the information, such the information, such and to avoid collected spreadsheet, a ble to ensure licenselements are required. Response Mitigate CO 27001 certification are in place to misses that the vendor sevendor's own docu ionally recognized fare stated to have be misses that the vendor with the vendor's own docu ionally recognized fare stated to have be misses that the vendor's with the vendor's own docu ionally recognized fare stated to have be misses that the vendor's with the vendor's own documents of the vendor's own documents own documents own documents own documents	cting SIN within s this data is required ing revenue and red as part of the Residual Risk 3 - Medium Ion as well as a tigate privacy and ris heavily reliant on mentation and rameworks and open put in place are		
Risk Weak or absence of technical security controls Use of third-party	SIN number or Electronic Infor UBC databases The project has Sophia. This wil as part of the ir correct tax slips invention disclosed and the second of the security risks. The vendor has completed HEC security risks. The AWS hostin internal process standards (e.g., acceptable for the second of	financial information (de mation Information Se which should remain the sagreed to limit collection II be collected and retain exercise are created. Other persosure process. Inherent Likelihood 4 - High The provided security attest EVAT. These documents of the information contained geld platform for security coses suggest that they strictly. ISO, NIST). Per the HECK use at UBC. 4 - High The provided a third the sagnetic strictly attests and the strictly attests at UBC.	emed Very High Risk, curity Standard U1). To sole repository of such that is sole repository of UBC Accounts Paya onal information data Inherent Impact 4 - Major Inherent Impact 4 - Major ations in the form of light that is sole repository of the HECVAT suggestion of the HECVAT suggestion of the HECVAT suggestion of the HECVAT, the controls that is sole repository of the repository	his data should be on the information, such the information, such and to avoid collected spreadsheet, a ble to ensure licenselements are required. Response Mitigate CO 27001 certification at are in place to misses that the vendor sevendor's own docu ionally recognized fare stated to have be misses that the second to have be misses that the se	cting SIN within s this data is required ing revenue and red as part of the Residual Risk 3 - Medium On as well as a tigate privacy and is heavily reliant on mentation and rameworks and open put in place are 3 - Medium		
Risk Weak or absence of technical security controls Use of third-party applications with	SIN number or Electronic Infor UBC databases The project has Sophia. This wil as part of the ir correct tax slips invention disclosed and the second of the invention disclosed and the second of the security risks. The end of the second of	financial information (de mation Information Se which should remain the sagreed to limit collection of the collected and retain mention disclosure and for are created. Other personance of the collected source process. Inherent Likelihood 4 - High These documents of the information containe galatform for security coses suggest that they strictly CISO, NIST). Per the HECV use at UBC. 4 - High The completed a third cyclosely, and continue to the completed at third cyclosely, and continue to the which should be seen to the complete of the collection of the coll	emed Very High Risk, icurity Standard U1). To sole repository of such that is sole repository of under the sole in the form of the such that is sole in the HECVAT suggestant of the HECVAT suggestant o	his data should be on the information, such and to avoid collect of the spreadsheet, a ble to ensure licenselements are requised. Response Mitigate CO 27001 certification are in place to misest that the vendor vendor's own docuionally recognized fare stated to have be stated to have but to ensure adequations.	cting SIN within s this data is required ing revenue and red as part of the Residual Risk 3 - Medium On as well as a tigate privacy and is heavily reliant on mentation and rameworks and open put in place are 3 - Medium		
Risk Weak or absence of technical security controls Use of third-party applications with	SIN number or Electronic Infor UBC databases The project has Sophia. This wil as part of the ir correct tax slips invention disclosed and the second of the invention disclosed and the second of the second of the security risks. The AWS hostin internal process standards (e.g., acceptable for the second of the	financial information (de mation Information Se which should remain the sagreed to limit collection II be collected and retain exercise are created. Other persosure process. Inherent Likelihood 4 - High The provided security attest EVAT. These documents of the information contained geld platform for security coses suggest that they strictly. ISO, NIST). Per the HECK use at UBC. 4 - High The provided a third the sagnetic strictly attests and the strictly attests at UBC.	emed Very High Risk, icurity Standard U1). To sole repository of such that is a sole repository of UBC Accounts Paya onal information data a sole of the sol	his data should be on the information, such and to avoid collect of the spreadsheet, a ble to ensure licenselements are requised. Response Mitigate CO 27001 certification are in place to misest that the vendor vendor's own docuionally recognized fare stated to have be stated to have but a stated to have but a stated to have but a stated to the consure adequatandards.	cting SIN within s this data is required ing revenue and red as part of the Residual Risk 3 - Medium Ion as well as a tigate privacy and is heavily reliant on mentation and rameworks and been put in place are 3 - Medium		
Risk Weak or absence of technical security controls Use of third-party applications with	SIN number or Electronic Infor UBC databases The project has Sophia. This wil as part of the ir correct tax slips invention disclosed and the second of the invention disclosed and the second of the second of the security risks. The AWS hostin internal process standards (e.g., acceptable for the second of the	financial information (de mation Information Se which should remain the sagreed to limit collection of the collected and retain mention disclosure and for are created. Other personance of the collected source process. Inherent Likelihood 4 - High These documents of the information containe galatform for security compared to the collected at the collected at UBC. 4 - High The collected and retain the collected at the collected at the collected at third collected at third collected at the	emed Very High Risk, icurity Standard U1). To sole repository of such that is a sole repository at the sole repository of the sole reposito	his data should be on the information, such and to avoid collect of the spreadsheet, a ble to ensure licenselements are requised. Response Mitigate CO 27001 certification are in place to misest that the vendor vendor's own docuionally recognized fare stated to have be stated to have but a stated to have but a stated to have but a stated to the consure adequatandards.	cting SIN within s this data is required ing revenue and red as part of the Residual Risk 3 - Medium Ion as well as a tigate privacy and is heavily reliant on mentation and rameworks and been put in place are 3 - Medium		

Figure 4 - Risk Mitigation Table



2.3 Collection Notice

A standard UBC collection notice is required to be implemented when personal information is collected. A sample follows:

Your personal information is collected under the authority of section 26(c) of the Freedom of Information and Protection of Privacy Act (FIPPA). This information will be used to manage your relationship with UBC in the context of invention and patent disclosures. Questions about the collection of this information may be directed to XXXXX@ubc.ca.

It is advised that the FIPPA-required privacy notification be presented to the individual when they submit their invention disclosure, or when they register and provide their personal information.

2.4 Consent for Storage/Access Outside of Canada & Opt-Out Procedure (If Any) Not required.

2.5 Consent Withheld Procedure

Not applicable.

PART 3: SECURITY OF PERSONAL INFORMATION

3.1 Physical Security Measures

This project is required to comply with UBC Policy SC14 (Information Systems Policy) and applicable UBC ISS (Information Security Standards).

3.2 Technical Security Measures

This project is required to comply with UBC Policy SC14 (Information Systems Policy) and applicable UBC ISS (Information Security Standards).

3.3 Security Policies, Procedures, and Standards

This project is required to comply with UBC Policy SC14 (Information Systems Policy) and applicable UBC ISS (Information Security Standards).

UBC has had limited visibility into or access to Wellspring's own information security policies, practices, or standards. Publicly available information, as well as detailed provided by the vendor, including a HECVAT report, asserts that Wellspring employs acceptable standards and practices in line with global standards and frameworks; however, these assertions could not be substantiated as no third-party attestation has been completed. This has been noted in the risks table.

3.4 Tracking Access / Access Controls

Access should be granted to individuals on a need to know basis only. Users will have access to the system to submit invention disclosures and contract requests. They can also log in to see information related to their own submissions. Only UBC UILO staff will have access to full data. At UBC, this is a permission defined by the organization. In general, this is limited to UILO staff. At Wellspring, Operations and Engineering have access to personal information, and this is limited to: name, address phone and e-mail.



PART 4: ACCURACY, CORRECTION, AND RETENTION

4.1 Updating and Correcting Personal Information

Personal information may be updated by individuals whose personal information has been collected contacting the UILO, as required.

4.2 Decisions That Directly Affect an Individual

This project captures personal information that directly affects an individual and would be required to be retained for at least one year under s.(31) of FIPPA.

4.3 Records Retention and Disposal

This project is required to comply with UBC Records Management Policies.

The project has not developed a defined records retention plan and is encouraged to do so. The vendor has noted that data retention procedures are dependent on data type and can be changed based on client requirements. This has been noted in the risks table.

PART 5: FURTHER INFORMATION

5.1 Systematic Disclosures of Personal Information

This project does not involve the systemic disclosure of personal information. However, some data elements are shared with other UBC units (e.g., Finance) to enable payments.

5.2 Access for Research or Statistical Purposes

This project does not involve the disclosure of personal information for research or statistical purposes as contemplated under s.(35) of FIPPA.

5.3 Other Applicable Legislation and Regulations

This project is not subject to other applicable legislation or regulations.



PART 6: ACCESS AND PRIVACY MANAGER COMMENTS

6.1 Information or Materials Reviewed

Overall, the information provided was deemed reasonable to provide an understanding of operating privacy and security controls.

Information Reviewed	Date Received
HECVAT302_Full_Sophia.xlsx	2023-06-02 21:16:45
ISO 27001 Controls List.xlsx - ISO	2023-06-02 21:22:12
Control Domains.pdf	
RE_ Comment added to_ Wellspring	2023-06-02 21:16:45
Sophia - Technology Management	
System (#INC2749520).msg	
Security	2023-06-02 21:22:12
Statement_Template_Sophia_2021.doc	
x.pdf	
SOC 2 - AWS SOC 2 Report 2021	2023-06-02 21:22:14
FINAL.pdf	
SOC_Continued_Operations_Letter.pdf	2023-06-02 21:22:13
Sophia Diagram (AWS CA) (1).jpg	2023-06-02 21:17:54
Sophia Diagram (AWS CA) (1).pdf	2023-06-02 21:16:44
Sophia Diagram (AWS CA).pdf	2023-06-02 21:22:11
UBC_MLSA_WW_V4-Clean.pdf	2023-06-02 21:22:14
Wellspring Worldwide - ISO 27001	2023-06-02 21:16:45
Certificate - 2022.pdf	
Wellspring Worldwide Incorporated ISO	2023-06-02 21:22:13
27001 Certificate-with signature-1-2-	
1.pdf	

6.2 Analysis and Findings

Based on the information provided, our review has concluded there are no significant privacy or security risks introduced by this project or use-case. The project may proceed in the proposed manner as long as it continues to fully comply with the FIPPA legislation and the UBC Information Security Standards, subject to the conditions of approval in the next section.

6.3 Conditions of Approval

None Specified.



6.4 Review and Distribution

This refers to the report approval process. The Owner is accepting the accuracy of the data provided to PrISM for this review and the risk responses. The Owner is responsible for the on-going operational activities and must ensure that this project continues to meet legislative and legal requirements, along with Information Systems Policy (SC14) requirements. Any change in PI collection or use will require new PIA.

Assessment Acceptance

John-Paul Heale

This refers to the report distribution, including Requestor, Project Manager, Owner, and assigned Risk Advisor.

Distributed To

Requestor: William Sharp, Associate Director, Technology Transfer
Project Manager: William Sharp, Associate Director, Technology Transfer
Owner: Mark John-Paul Heale, Managing Director, University Industry Liaison
Risk Advisor: Christian Stockman, Senior Advisor, Privacy and Information
Security Risk

PIA Request History:

PIA Request Date	Report Created
2022-04-04 10:47:03	2023-06-02 16:14:37