PIA01011 – Survey Monkey Apply

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
Pimkae Saisamorn	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	2021-10-28	Pimkae Saisamorn	Report Creation

Figure 2 - Document Revision History and Revision Summary

TEMPLATE REVISION APPROVAL

REVISION #	DATE	REVISED BY	DESCRIPTION
1.00	2021-10-28	Dmitriy Ryabika	Initial release of document

Figure 3 - Major Document Revision Approval History

TABLE OF CONTENTS

TABLE OF FIGURES

PART 1: GENERAL INFORMATION & OVERVIEW

1.1 Executive Summary

SurveyMonkey Apply is a Software as a Service, developed and supported by SurveyMonkey. The software streamlines the collection, submission, score, rank, feedback processes. It eliminates the need of paper-based application and document submission. It does not integrate with any UBC systems apart from CWL integration.

SurveyMonkey Apply operations are headquartered in the Ottawa office of SurveyMonkey which staffs approximately 180+ of the company's global population of about 1300+ employees across offices in San Mateo, Portland, Seattle, New York, Ottawa, London, Berlin, Sydney, Amsterdam, and Dublin. It is noted that during the implementation stage, a main point of contact and the implementation specialist responsible for getting the platform up and running was based in Toronto and worked on Canada-based servers to setup the site for UBC.

The project initially planned to engage with a US-based email processor, Sparkpost, to send notification and communication channel with candidates. However, it has subsequently changed the email processor using UBC mail system. SM Apply's primary data center is provisioned through iWeb, the hosting provider, and is located in Quebec, Canada. The data is stored on dedicated servers and infrastructure owned and managed by SurveyMonkey. iWeb provides physical and environmental controls.

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

The UBC VP Research and Innovation (VPRI) is looking to implement to SurveyMonkey Apply (SM Apply) to administer internal funding applications and provide consistent experience across all competitions, simplify application process for applicants, and standardize administration and adjudication of these competitions.

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 - Medium

1.3 Scope of PIA

The scope of this PIA is the implementation of SurveyMonkey Apply for direct use by UBC faculty, staff, students and other third parties who are authorized to use these products and services on behalf of UBC.

1.4 Related PIAs

Not applicable.

1.5 Elements of Information or Data

Applicant data includes last name, first name, email, phone number, application details and other common questions associated with a grant application.

Additional data will include the names of internal and external reviewers, their contact information, application scores, application feedback, decisions (funded/not funded), possibly images or videos.

Individual will have to enter and/or verify their contact details, their current appointment, and other information needed for grant application.

The project pre-fills some information ourselves, for example, data on external reviewers for a grant (consultants or faculty members from other universities) so that the data is in a centralized repository.

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

SurveyMonkey Apply servers storing UBC data are hosted at iWeb in Canada. However, SurveyMonkey technical support team can potentially come from offices across continents located outside of Canada. This observation is included in the risk mitigation table.

1.7 Data-Linking Initiative

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

1.8 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

No Applicable.

2.2 Risk Mitigation Table

Category: Security					
Risk	**Ref#**	**Inherent Likelihood**	**Inherent Impact**	**Response**	**Residual Risk**
Retaining PI longer than necessary	RK0020192	4 - High	3 - Significant	Mitigate	3 - Medium
	Mitigation Plan: With the potential implementation of the eligibility (screening) questions such as historical exclusion criteria, the project to update the existing data retention policy to include the relevant changes in accordance with the appropriate retention schedule and data destruction policies as set out by the UBC RMO.				
Inadequate third-party information sharing controls	RK0020043	4 - High	4 - Major	Mitigate	3 - Medium
	Mitigation Plan: The project to arrange with the external reviewers to sign on the Security and Confidentiality Agreement (SACA) or another agreement that contains equivalent requirements before they are given access to personal or otherwise confidential/sensitive information held by UBC and they must agree to protect any information they may access and to comply with the FIPPA legislation. During the course of our review, we noted that the project has developed and implemented an agreement for the external reviewers to sign.				
PI stored / accessible outside of Canada	RK0020190	4 - High	4 - Major	Mitigate	3 - Medium
	Mitigation Plan: The project to work with SurveyMonkey Apply and Sparkpost to implement following actions to address the disclosure of PI outside Canada concerns: 1. Arrange a temporary-only access to the support team which is based outside Canada within the minimum period of time necessary to complete the implementation, maintenance and trouble-shoot. 2. Set up SMTP using UBC mail system and ensure that no emails be routed outside Canada. During the course of our review, we noted that the project has implemented the recommended risk mitigation items listed above.				
Category: Security					
Weak or absence of administrative security controls	RK0020302	4 - High	4 - Major	Mitigate	3 - Medium
	Mitigation Plan: The project to inquire about the most recent SOC review and obtain the SOC report of iWeb hosting provider to ensure the physical security controls of iWeb is adequate. During the course of our review, we noted that the project has reached out to the vendor to obtain the updated SOC report.				
Use of third-party applications with inadequate controls	RK0020191	4 - High	3 - Significant	Mitigate	3 - Medium
	Mitigation Plan: The project to work with SurveyMonkey Apply to include following key privacy provisions in the contract agreement to address privacy risks. • personal information collected without authorization (i.e., collection/use for the purposes beyond a UBC program or activity (i.e. the vendors purposes)) • Personal information stored outside Canada (e.g. using cloud services) (i.e., Specific provisions on storage in Canada) • Personal information disclosed without authorization (i.e., disclosure to subcontractors or third parties without suitable contractual protections) • Personal information not stored long enough / too long (i.e., destruction at contract termination/at request) During the course of our review, we noted that the contract agreement has been established and incorporated with the suggested provisions.				

Figure 4 - Risk Mitigation Table

2.3 Collection Notice

Applicants are given a standard personal information collection notice before they provide their personal information. This discloses the legal authority to collect information, the purpose for collection, and contact information for asking for clarification.

2.4 Consent for Storage/Access Outside of Canada & Opt-Out Procedure (If Any)

Consent is not required as use of [Insert Tool] will not result in the storage of personal information outside Canada.

2.5 Consent Withheld Procedure

Not applicable. Consent is not required.

PART 3: SECURITY OF PERSONAL INFORMATION

3.1 Physical Security Measures

iWeb provides physical and environmental controls. The 2018 SOC report of iWeb did not note any major exceptions whereas the iWeb management had agreed and implemented the corrective actions. In addition, the bridge letter issued on December 12, 2019 did confirm that there were no updates or changes to the internal controls of iWeb. However, our concern is a review gap from January 2020 to-date as we do not know what might have been changed. This observation is included in the risk mitigation table.

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). The VPRI is requesting for a separate instance and will be sole user of the system.

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).

3.4 Tracking Access / Access Controls

SurveyMonkey Apply is set up with CWL integration. The collected information will only be accessible to VPRI Office staff directly involved in competitions management (~5 people). The applicants will only see the applications they created (current and previous). Reviewers will only have access to the limited set of applications they are responsible for 24 hours prior to the adjudication panel. All reviewers receive access to all applications for transparency purposes; access is then revoked upon reaching the final funding decisions. Only SurveyMonkey staff have access to UBC data and no subcontractors are used.

PART 4: ACCURACY, CORRECTION, AND RETENTION

4.1 Updating and Correcting Personal Information

The applicants are responsible for entering and updating their personal information. The project only uses the populated information to provide an approval on any grant applications.

4.2 Decisions That Directly Affect an Individual

SurveyMonkey Apply enables VPRI to streamline the application process and capture relevant data in a systematic way. The information stored in SurveyMonkey apply will be used for review and provide comments and scores, and finally make decisions to provide the funds.

4.3 Records Retention and Disposal

The VPRI follows the data retention schedule "Research Grants Records – Grant Applications 005-04" (https://recordsmanagement.ubc.ca/files/2014/09/sched_5-04.pdf). Individual scores and reviewer comments are deleted upon completion of adjudication and notification of applicants. Applicants are sent a summary file with these comments and overall scores. Once these files are sent, there is no longer a need to retain the raw information within the VPRI.

PART 5: FURTHER INFORMATION

5.1 Systematic Disclosures of Personal Information

This project does not involve the systemic disclosure of personal information. The information stored in SurveyMonkey Apply is disclosed to the reviewers and rarely to joint funding competitions. The VPRI staff have access to the information for administrative supports in completing the application process.

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 provided information was deemed reasonable to provide an understanding of operating privacy and security controls and allow us to assess the mitigated risks and recommend the risk mitigation plan to ensure that the residual risks are managed at an acceptable level:

6.2 Analysis and Findings

Based on our understanding of the collection, use, disclosure, and retention of personal information, our review noted the key privacy and information security risks and the risk mitigation plan is recommended and provided to the project. The project has agreed and implemented the recommended remediate actions as outlined in the risk mitigation plan to minimize risk exposures and to comply with the FIPPA requirements and UBC Information Security Standards.

6.3 Conditions of Approval

Our review has concluded that there are no significant privacy or information security risks introduced by this project however we do recommend the project ensure that it continues to fully comply with the FIPPA legislation and the UBC Information Security Standards.

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
Dmitriy Ryabika

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

Distributed To
Requestor: Dmitriy Ryabika, Research Manager **Project Manager:** Dmitriy Ryabika, Research Manager **Owner:** Dmitriy Ryabika, Research Manager **Risk Advisor:** Pimkae Saisamorn, Senior Information Security Risk Analyst

PIA Request History:

PIA Request Date	Report Created
2020-06-01 08:59:09	2021-10-07 18:54:17