PRIVACY IMPACT ASSESSMENT (PIA)
CLOSURE SUMMARY

Initiative	SmartSheet
PIA Reference #	2024-001
PIA Completion Date	_____, 2024
Project Sponsor	Applied Research and Technology Services
Unit	Applied Research and Technology Services

The purpose of a PIA is to determine whether an initiative complies with the *Freedom of Information and Protection of Privacy Act* ("**FIPPA**") and JIBC's policies and procedures. This document is to advise that the PIA review of this initiative has been completed. The following outlines the scope, issues, legal basis and conclusions associated with this PIA.

Initiative Description & Scope

SmartSheet is an application that enables teams to manage projects, automate processes and scale programs in a single platform.

Information Reviewed

Our review is based primarily on the PIA Questionnaire, completed by Annette Hurley, which is attached at Schedule A. We also spoke with Technology Services to verify certain assumptions about the application, particularly where any personal information may be stored and whether the application is cloud-based or uses a closed system.

Legal Basis - Privacy

According to the PIA Questionnaire, the proposed tool may collect information related to bio/demographic information, academic/education information, employment information, images, opinions, business contact information and personal contact information of applicants, students and employees.

Such information is permitted to be collected pursuant to section 26(c) of FIPPA, which states that a public body may collect personal information if the information relates directly to and is necessary for a program or activity of a public body. Pursuant to section 27(2) of FIPPA, a public body must ensure that an individual from whom it collects personal information is told: (a) the purpose for collecting it; (b) the legal authority for collecting it; and (c) the contact information of an officer or employee of the public body who can answer the individual's questions about the collection. It is unclear if users are currently presented with a collection notice that meets this requirement.

Pursuant to section 32(a) of FIPPA, a public body may use personal information in its custody or under its control for the purpose for which the information was obtained, or compiled, or for a use consistent with that purpose.

Pursuant to section 33(2)(d) of FIPPA, a public body may disclose personal information for the purpose for which the information was obtained or compiled, or for a use consistent with that purpose.

Pursuant to section 34 of FIPPA, a use or disclosure of personal information is consistent with the purpose for which the information was obtained or compiled if the use: (a) has a reasonable and direct connection to that purpose; and (b) is necessary for performing the statutory duties of, or for operating a program or activity of, the public body that uses or discloses the information.

Section 33.1 of FIPPA requires additional analysis be conducted when personal information will be stored outside of Canada. In particular, we are required to consider factors such as whether the personal information is sensitive, where and how the information is stored, the likelihood of unauthorized access, and the impact to the individual of such an event.

Current guidance from the Province of British Columbia suggests that sensitive personal information includes, but isn't limited to:

- Personal health information
- Genetic and biometric data
- Personal financial information
- Geolocation data
- Criminal records
- Racial or ethnic origin
- Sexual orientation
- Religious, philosophical or political beliefs

The nature of the personal information that is collected with respect to the use of this proposed tool does not appear to be inherently sensitive. As such, we are not required to proceed with a supplementary assessment.

Legal Basis - Security

Pursuant to section 30 of FIPPA, a public body must protect personal information in its custody or under its control by making reasonable security arrangements against such risks as unauthorized collection, use, disclosure or disposal. Personal information will likely be stored outside of Canada. However, Technology Services has confirmed that the application uses robust security measures, including encryption for all data in transit and at rest, as well as regular security scans and penetration tests of their infrastructure:

https://www.smartsheet.com/trust/security

Furthermore, JIBC has purchased the Enterprise tier of the service and will be configuring single sign-on within Azure.

Conclusions

Based on the information provided, our review has concluded that the proposed tool may be used for its intended purpose.

Responsibilities

Technology Services are responsible for ensuring that individuals are informed that we will be collecting personal information about them. Here is a sample form of collection notice that could be used:

> "Your personal information is collected under the authority of section 26(c) of the *Freedom of Information and Protection of Privacy Act*. This information may be used by JIBC as for **[insert purpose of collection.]**. If you have any questions about the collection of this information, please contact privacy@jibc.ca."

Furthermore, Technology Services are responsible for Informing the General Counsel of any material omissions or inaccuracies in the information relied upon in this PIA, and submitting to the General Counsel a new PIA request if there are any significant changes to this initiative.

If you have any questions or concerns about this PIA, please contact the General Counsel.

SCHEDULE A
PIA QUESTIONNAIRE

Please see attached.

Justice Institute
BRITISH COLUMBIA

LEARNING THAT TAKES YOU BEYOND

PRIVACY IMPACT ASSESSMENT QUESTIONNAIRE

for

SmartSheet

1. Purpose of the Privacy Impact Assessment Questionnaire

This form is used by JIBC to provide a high-level overview of the potential privacy risks of a current or proposed policy, system, project, program or activity. The results of these screening questions help judge the level of potential risk, the extent to which risk mitigation strategies may be needed and when completion of a privacy impact assessment is required under the *Freedom of Information and Protection of Privacy Act* (British Columbia) (the "**Act**").

2. Privacy Questions

Questions	Answers
Does the program involve personally identifiable information (PII) (as defined by the Act)? [Y/N]	Y
Will the program involve the collection or creation of new information about individuals? [Y/N]	Y
Will personal information about individuals be disclosed to organizations, programs, processes or people who have not previously had routine access to the information? [Y/N]	N
Will personal information about individuals be used for a purpose it is not currently used for, or in a way it is not currently used? [Y/N]	N
Will the program require contacting individuals in ways that they may find intrusive? [Y/N]	N
Does the program have a collection notice or use policy? [Y/N]	Y - https://www.smartsheet.com/legal/privacy

3. Technology Questions

Questions	Answers
Does this program involve the implementation of a new electronic system or use of a new application or software to support the creation, collection, updating or storing, backing-up or disposition of personal information? [Y/N]	Y
Does this program require any modifications to existing information technology (IT) systems (e.g., integration with or consolidation of other IT systems)? [Y/N]	N
Will a new or modified electronic system change the existing business workflow? [Y/N]	N

Does the program involve the use of new technology that might be perceived as being privacy intrusive? [Y/N]	N

4. Impact Questions

Questions	Answers
What are the purpose of collection, use and/or disclosure of the personal information? [Internal/External/Both]	Internal
Will personal information about the same individual that was previously maintained separately now be aggregated and stored together? [Y/N]	Y
How would you describe the information classification level of the personal information? (Select all that apply) • Highly Confidential • Confidential • Public	Confidential
What are the type(s) of personal information? (Select all that apply) • Bio/demographic information • Academic/education Information • Employment information • Medical/health Information • Financial Information • Criminal information • Images • Opinions about individuals • Individuals' personal views and opinions • Business contact information • Personal contact information • Other	
What are the type(s) of individuals? (Select all that apply) • Prospects • Applicants • Students • Employees • Donors/alumni/other 3rd parties	

• Volunteers • Service providers • Other	
How many records documenting individuals will be stored, accessed, used or disclosed? [1-1000], [1001-5000], [5,001-50,000], [50,001-100,000], [100,000+]	
How many JIBC employees, volunteers and service provider employees will be able to access, collect, use or disclose the information? [1-10], [11-50], [51-100], [101-250], [251-500], [501-1,000], [1,000+]	
Is any of the information owned by another organization? [Y/N]	N

5. Probability Questions

Questions	Answers
Where will the information be stored? (Select all that apply) • [redacted] [redacted] S.15(1)(l) [redacted] [redacted]	
Is any of the information accessed from outside of Canada? [Y/N]	N
Will personal information be transmitted? (Select only one) • Personal information is used in a closed system (i.e., no connections to the Internet, Intranet or any other system and the circulation of hardcopy documents is controlled) • Personal information is used in a system that has connections to at least one other system • Personal information is transferred to a portable device (i.e., USB key, diskette, laptop computer), transferred to a different medium or is printed • Personal information is transmitted using wireless technologies	
Will a third party (e.g., vendor or service provider) have access to the information? [Y/N]	N
Will the program result in different record keeping systems converging? [Y/N]	N