Justice Institute
BRITISH COLUMBIA

LEARNING THAT TAKES YOU BEYOND

PRIVACY IMPACT ASSESSMENT (PIA)
CLOSURE SUMMARY

Initiative	Wrike Project Management Software
PIA Reference #	2025-xxx
PIA Completion Date	November ___, 2025
Project Sponsor	Birender Singh – Project Manager, Enterprise Systems
Unit	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

The initiative involves the ongoing use of Wrike, a cloud-based project management and workflow coordination tool used by various JIBC administrative teams and service providers. The platform supports collaborative task tracking, project planning, and resource coordination.

Wrike will be used by employees and certain service providers. The information entered into the system consists primarily of business contact information, employment-related information, and limited personal contact details associated with user accounts. No sensitive personal information, such as medical, financial, biometric, or student academic records, will be collected or stored within the system.

No changes to existing business workflows or data uses are contemplated.

Information Reviewed

Our review is based on the completed PIA Questionnaire (attached as Schedule A) and additional information provided by Technology Services, including:

- Confirmation that standard SSO and authentication controls have been implemented
- Review of Wrike's publicly available security documentation
- Confirmation from TS that no material security concerns were identified

Legal Basis - Privacy

Collection

The PIA Questionnaire confirms that Wrike collects limited personal information that is required to administer user accounts and support collaboration, including:

- Employee employment information (e.g., name, position, role in a project)
- Business contact information
- Occasional personal contact information where voluntarily provided

This collection is authorized under section 26(c) of FIPPA, as the information relates directly to and is necessary for managing JIBC's operational projects and internal workflows.

Wrike does not involve the creation of new personal information beyond what already exists within JIBC administrative systems, nor does it introduce new categories of personal information.

The platform already includes a general use policy and collection notice in its onboarding materials.

Use & Disclosure

Use and disclosure of personal information for project coordination, workflow management, and communication is permitted under:

- Section 32(a) – use for the purpose for which the information was obtained
- Section 33(2)(d) – disclosure for a consistent purpose
- Section 34 – "consistent purpose" defined as reasonably and directly connected to the original purpose and necessary to operating a program or activity

No disclosure of personal information to new or previously unrelated parties is anticipated.

Wrike support personnel may have limited access to user information for troubleshooting. This is consistent with the original purpose of collection and is standard for SaaS platforms.

Cross-Border Considerations

Wrike stores data outside of Canada. Under section 33.1 of FIPPA, this necessitates an assessment of sensitivity, storage architecture, likelihood of unauthorized access, and harm.

The personal information involved is employment-related and low sensitivity, consisting primarily of names, roles, and business contact details. It does not include medical, financial, biometric, student, or other high-risk categories.

Given the nature of the data and Wrike's published security practices, a supplementary risk assessment under section 33.1 is not required.

If Wrike is ever used to store sensitive or student-related information, a renewed PIA is required.

Legal Basis - Security

Under section 30 of FIPPA, JIBC must ensure reasonable security measures are in place.

Technology Services has confirmed:

- SSO and standard authentication measures have been implemented
- Wrike's platform-level security controls appear sound
- No major risks were identified

Wrike's published security documentation indicates:

- Encryption of data in transit and at rest
- Access controls, firewalls, and intrusion detection
- SOC 2 and ISO-related security frameworks
- Physical and logical safeguards appropriate to cloud platforms

Wrike connects to other systems only through limited integrations, such as Workato, and no sensitive internal systems are involved. Only non-sensitive administrative data is stored.

Data may be accessed by Wrike personnel for technical support, but no routine access is expected.

Conclusions

Based on the information provided, our review has concluded that the Wrike Project Management Software may be used for its intended purpose, provided that:

- Personal information entered into the system remains limited to employment and business contact information
- Sensitive personal information (e.g., health, financial, student academic data) is not stored in Wrike
- Any material changes to the scope of use, data types, or system functionality trigger a renewed PIA review

Responsibilities

The program area is responsible for:

- Ensuring employees understand the type of information to be entered into Wrike
- Ensuring that no high-risk or sensitive personal information is stored in the platform
- Notifying the General Counsel if Wrike's use expands or if new categories of personal information are proposed to be added

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

SCHEDULE “A”
PIA Questionnaire

Please see attached.

PRIVACY IMPACT ASSESSMENT QUESTIONNAIRE

for

Wrike – Project Management Software

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]	N
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

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]	N
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]	Wrike both collects and processes personal information, uses it for service needs.
Will personal information about the same individual that was previously maintained separately now be aggregated and stored together? [Y/N]	N
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	• Employment information • Potential Personal contact • Business contact information
What are the type(s) of individuals? (Select all that apply) • Prospects • Applicants • Students • Employees • Donors/alumni/other 3rd parties • Volunteers • Service providers	• Employees • 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+]	1-1000
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+]	51-100
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) • On campus – JIBC servers • On campus – other • Off-campus – inside Canada • Off-campus – outside Canada	Off-campus – outside Canada
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	Personal information is used in a system that has connections to at least one other system (Workato)
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