Privacy Impact Assessment for Ministries

PART 1: GENERAL INFORMATION

JIBC PIA Number: 2023-003

Initiative title:	Zoom
Your name and title:	Pete Learoyd
Your email address:	plearoyd@jibc.ca
Program/Department Manager	Sarah Wareing
Email address	swareing@jibc.ca
Chief Privacy Officer:	Derek Deacon, General Counsel
CPO email address:	ddeacon@jibc.ca

Your CPO will complete the questions in the table below.

FOR CPO USE ONLY
Is this a PI or non-PI assessment?
PI
Is this initiative a data-linking program under FOIPPA?
No
Is this initiative a common or integrated program or activity under FOIPPA?
No
Related PIAs, if any:
No
Does this initiative involve disclosures of sensitive personal information outside of Canada?
No

1. What is the initiative?

A Zoom Meeting refers to a video conferencing meeting that's hosted using Zoom. When users join these sessions, they are given the option to turn on their webcam or microphone. Sessions can potentially be recorded by the meeting host (the recording function will not be blocked by JIBC). Sessions can be enabled for both desktop and mobile applications. Zoom meetings can be synced to calendars, and users delivering the session can upload an image to customize their background. Regarding Zoom support, it is expected that support of Zoom by JIBC TS will be focused on user administration, connectivity and support of users to be able to connect into a session. This may include the Windows/Mac app, web-based interfaced or mobile app. Being a cloud-based service, most of the support solutions will be leveraging from the information and tools provided by Zoom. Zoom offers Outlook application plugins for meeting joining and meeting/session creation.

2. What is the scope of the PIA?

The scope of this PIA is limited to the use of Zoom products in its Canadian based configuration.

3. What are the data or information elements involved in your initiative?

Information Collected using Zoom

The information collected using Zoom varies dramatically depending on whether the individual is an account holder. While you must be an account holder to host a meeting, you do not need to have an account to participate in one. JIBC holds an enterprise license and makes accounts available to faculty and staff members upon request.

Information Type	Information Collected from Account Holder	Information Collected from Non-Account Holder
Identifiers	Name, username, physical address, email address, phone numbers, and other similar identifiers	Username
Information about job	e.g. job title, employer	N/A
Facebook profile information	Facebook profile information (when you use Facebook to login to the service or to create an account*	N/A
General information	General information about your product and service preferences	N/A
Device and network information	Information about your device, network, and internet connection, such as your IP address(es), MAC address, other device ID (UDID), device type, operating system type and version, and client version	Information about your device, network, and internet connection, such as your IP address(es), MAC address, other device ID (UDID), device type, operating system type and version, and client version
Usage information	Information about your usage of or other interaction with the service	Information about your usage of or other interaction with the service

Customer content	Other information you upload, provide, or create while using the service	Other information you upload, provide, or create while using the service

Information discussed by the participants during the session flows through the Zoom servers, but is not collected by Zoom as the cloud recording feature has been disabled. If the meeting host activates the local recording option, the recordings will be stored on the host's computer. All participants will receive an automatic notification when recording is enabled.

Information Provided by Zoom to Third Parties

Zoom, its third-party service providers, and advertising partners (e.g., Google Ads and Google Analytics) automatically collect some information about users when you use Zoom, using methods such as cookies and tracking technologies. Information automatically collected includes Internet protocol (IP) addresses, browser type, Internet service provider (ISP), referrer URL, exit pages, the files viewed on the Zoom site (e.g., HTML pages, graphics, etc.), operating system, date/time stamp, and/or clickstream data. Zoom's Privacy Policy states that it uses this information to offer and improve our services, trouble shoot, and to improve its marketing efforts. While the disclosed data is not linked to a username, it is potentially reidentifiable through the mosaic effect.

3.1 Did you list personal information in question 3?

Personal information is any recorded information about an identifiable individual, other than business contact information. Personal information includes information that can be used to identify an individual through association or reference.

Yes.

- If yes, go to Part 2

PART 2: COLLECTION, USE AND DISCLOSURE

This section will help you to identify the legal authority for collecting, using, and disclosing personal information and to confirm that all personal information elements are necessary for the purpose of the initiative.

4. Collection, use, and disclosure

Typical Learning Use Case

Use this column to describe the way personal information moves through your initiative step by step as if you were explaining it to someone who does not know about your initiative.	**Personal Information**	**CPO fills in Collection, use, disclosure**	**CPO fills in FOIPPA authority**	**CPO fills in Other legal authority**
1. Instructor sends invitations to participate in Zoom session directly to students through JIBC's platform. No data stored by Zoom.	Students' email addresses	Use	32	
2. Student accepts invitation; login name is stored on Zoom server.	Login name (assuming it is personally identifiable	Collection	26(c)	

3. Metadata about session is stored on Zoom server.	Metadata of participant (assuming login name was personally identifiable)	Collection	26(c)	
4. If recorded, discussion is stored on Zoom server (if cloud recording turned on) or in the user's local storage (if cloud recording turned off).	Discussion may include personal information of the speaker or of third parties	Collection	26(c)	
5. Zoom administrators may monitor session, at JIBC's request, in order to install, implement, maintain, repair, troubleshoot or upgrade the system. No data stored.	Login name and metadata	Disclosure	33(2)(d)	

Typical Administrative Use Case

Use this column to describe the way personal information moves through your initiative step by step as if you were explaining it to someone who does not know about your initiative.	**Personal Information**	**CPO fills in Collection, use, disclosure**	**CPO fills in FOIPPA authority**	**CPO fills in Other legal authority**
1. Employee sends invitations to participate in Zoom session directly to other employees at their JIBC email addresses.	No personal information involved because email addresses of employees are not personal information.	N/A	N/A	
2. Employee accepts invitation; login name is stored on Zoom server.	No personal information involved because names of employees are not personal information.	N/A	N/A	
3. Metadata about session is stored on Zoom server.	Metadata of participant. (This is not personal information if work computer is used).	Collection, storage within Canada	26(c), 33(2)(d)	
4. If unrecorded, discussion flows through Zoom server without being stored there.	Discussion may include personal information of	Access within Canada	33(2)(d)	

Use this column to describe the way personal information moves through your initiative step by step as if you were explaining it to someone who does not know about your initiative.	Personal Information	CPO fills in Collection, use, disclosure	CPO fills in FOIPPA authority	CPO fills in Other legal authority
	the speaker or of third parties.			
5. If recorded, discussion is stored on Zoom server (if cloud recording turned on) or in the user's local storage (if cloud recording turned off).	Discussion may include personal information of the speaker or of third parties	Collection, storage within Canada	26(c), 33(2)(d)	
6. Zoom administrators may monitor session, at JIBC's request, in order to install, implement, maintain, repair, troubleshoot or upgrade the system.	Metadata	Access within Canada	33(2)(d)	

5. Collection Notice

All students are given a standard personal information collection notice when they apply for entry to JIBC. This discloses the legal authority to collect information, the purpose for collection, and contact information for asking for clarification. In practice, however, it is expected that most students will approach their instructor if they have any privacy questions about the use of Zoom. Such questions can be passed along to the CPO if necessary.

PART 3: STORING PERSONAL INFORMATION

If you're storing personal information outside of Canada, identify the sensitivity of the personal information and where and how it will be stored.

6. Is any personal information stored outside of Canada?

No.

- If no, go to Part 5

PART 5: SECURITY OF PERSONAL INFORMATION

This part captures information about the privacy aspects of securing personal information. People, organizations, or governments outside of your initiative should not be able to access the personal information you collect, use, store or disclose. You need to make sure that the personal information is safely secured in both physical (e.g., your office building or work environment) and technical (e.g., online cloud service) environments.

7. Does your initiative involve digital tools, databases or information systems?

No.

8. Are all digital records stored on government servers and are all physical records stored in government offices with government security?

No.

PART 6: ACCURACY, CORRECTION, AND RETENTION

In Part 6 you will demonstrate that you will make a reasonable effort to ensure the personal information that you have on file is accurate and complete.

9. How will you make sure that the personal information is accurate and complete?

It is the user's responsibility to ensure that any personal information that they provide in connection with the use of Zoom is accurate and complete.

10. Requests for correction

JIBC does not require the student to provide any personal information using Zoom. They can participate anonymously in a session if they wish. If they choose to provide personal information about themselves, they are responsible for ensuring the accuracy of their personal information. Zoom does not offer functionality to update or annotate personal information stored in its servers.

11. Does your initiative use personal information to make decisions that directly affect an individual?

No.

- If no, skip ahead to Part 7

PART 7: PERSONAL INFORMATION BANKS

A personal information bank (PIB) is a collection of personal information searchable by name or unique identifier.

12. Will your initiative result in a Personal Information Bank?

No.

PART 8: ADDITIONAL RISKS

13. Risk response

In the table below describe any additional risks that arise from collecting, using, disclosing, or storing personal information in your initiative that have not been addressed by the questions on the template.

Add new rows if necessary.

Possible risk	Response
Risk 1: Non-compliance with FIPPA requirement that personal information not be stored or accessible outside of Canada without consent.	Personal information stored in Canada. In administrative meetings, meeting hosts are advised not to record meetings where personal information is discussed. In learning sessions, students are advised of the option to anonymize themselves.
Risk 2: Non-compliance with FIPPA privacy notification requirement	All students receive a detailed privacy notification when they begin their studies at JIBC. Also, before each Zoom session, JIBC instructors are required to advise them in writing of their options to maintain anonymity.
Risk 3: Meeting organizers may not wish to have their information, including contact information, shared with Zoom	Guidance for faculty and staff in place. Faculty member names are not personal information as defined in FIPPA. Employees are not required to share any personal information during the session.
Risk 4: Users may already have the Zoom app and may wish to use it	Users who have downloaded the app have already consented to the terms of use. If they choose, they may uninstall the app and attend meetings without a Zoom account.

Possible risk	Response
Risk 5: Unauthorized interception or access to personal information transmitted by or stored in the system	Zoom has acceptable security controls in place. It uses end to end encryption and JIBC administrators will ensure that identified vulnerabilities have been patched. Also, if users follow JIBC guidance to turn off the record feature, no sensitive personal information will be collected and stored.
Risk 6: Meeting owner will share meeting recordings with unauthorized individuals	Instructors and staff receive privacy training. They are aware of the principles that govern the protection of privacy and the disclosure of personal information. Also, meeting recordings are unlikely to contain personal information.
Risk 7: Records are retained longer than required	Zoom does not allow recordings to be deleted until the account has been deleted. We have limited this risk by limiting the sensitivity of recorded information.
Risk 8: Users are not appropriately authenticated, leading to unauthorized access to personal information	Access to broadcast is via emailed invitation. However, any recipient can email the invitation to others without limitation. Program design, through limiting the sensitivity of recorded information, limits this risk.
Risk: 9: Faculty or staff may not have appropriate security controls in place if they are delivering classes while working remotely.	JIBC has guidance in place for remote working arrangements.
Risk 10: Vendor may change terms of use of the service.	JIBC will monitor the terms of use for changes.

Risk 11: Zoom may give or sell personal information to third parties	Zoom shares non-identifying metadata with service providers and advertisers. Students can mitigate (but not entirely eliminate) this risk by using a non-identifying name and by using privacy browser extensions to prevent third-party trackers from accessing their information.

[Approvals and Signatures to Follow]

PART 9: CHIEF PRIVACY OFFICER COMMENTS AND APPROVAL

Zoom does not store personal information outside of Canada. Zoom may be used for its intended purpose provided that JIBC utilizes the Zoom configuration through which personal information would only be stored within Canada.

Chief Privacy Officer	Signature	Date

PART 10: PROGRAM AREA SIGNATURES

Program/Department Manager	Signature	Date
Technology Services (only required if involved in preparing this PIA)	Signature	Date
Mike Proud Vice-President, Finance & Operations	Mike Proud Digitally signed by Mike Proud Date: 2023.12.13 09:52:08 -08'00' Signature	Dec13/23 Date