PRIVACY IMPACT ASSESSMENT
Zoom Video Conferencing

PIA REVIEW – EXECUTIVE REPORT

PIA 2020.03-051 ZOOM – V4

CONTRIBUTORS

CONTRIBUTOR	DEPARTMENT	POSITION
Tremonti, Robert	PrISM – Safety & Risk Services	Sr. Information Security Risk Analyst
Jay Loder	PrISM – Safety & Risk Services	Manager PrISM
Michael Lonsdale-Eccles	PrISM – Safety & Risk Services	Director PrISM – Safety & Risk Services
Hancock, Paul	Office of the University Counsel	Legal Counsel, Information and Privacy

PIA REVISION HISTORY

REVISION #	DATE	REVISED BY	DESCRIPTION
0.10	2020.03.17	Hancock, Paul	Review draft of PIA completed by PrISM
0.20	2020.04.02	Hancock, Paul	Finalize draft of PIA
0.30	2020.06.30	Loder, Jay	Updates to reflect transfer to Canadian hosting July 4, 2020
0.40	2020.09.15	Loder, Jay	Updates to reflect scope changes

BACKGROUND

Due to the COVID 19 crisis, UBC's PIA team has conducted a PIA under the oversight of the University Counsel to determine if Zoom video conferencing can be used at UBC to support remote learning and administrative uses. Zoom has been recommended by UBC's IT staff as it has been deemed to be the best fit to deliver on-line learning to UBC students, especially for very large classes.

This document intends to summarize the privacy risks and recommend mitigation strategies for those risks. The assessment is based on the information provided to the Privacy Matters team by the project implementation teams and UBC Procurement as of March 28, 2020, and subsequent information provided by Zoom and the project team. The PIA team has also reviewed security information provided by Zoom as well as publicly available information about Zoom security and privacy issues.

Zoom Video Communications provides remote conferencing services using a cloud-based Software as a Service (SaaS) platform. Zoom is headquartered in San Jose, California and uses cloud-based data centres around the world. In the standard configuration, data provided by users may be stored on any of these data centres. Zoom offers an option to store data in Canada, which UBC will use. This PIA is based on the storage in Canada configuration.

Zoom is able to provide video conferencing on a larger scale that some of its competitors such as Cisco WebEx, Google Teams and Skype. Zoom is currently used by many Canadian universities.

The following assumptions were considered in the drafting of this PIA:

- UBC has other video conferencing and messaging tools that can be used for sessions of up to 250 users, but Zoom is the only tool under consideration that is suitable for sessions with more than 250 users.
- UBC is planning to use Zoom for remote learning purposes as well as some administrative purposes, including sensitive purposes such as counselling and student advising. It is already being used by several other large educational institutions for these purposes.
- As far as we can determine, UBC's use of Zoom is hosted in Canada.
- As the recording feature is required by some instructors, UBC is not planning to block this feature.
- Zoom employees will not actively monitor any customer sessions unless we request them to do so for support or trouble-shooting purposes.

This Assessment is an evergreen document and as such, will be updated from time to time as additional services are reviewed, and where appropriate added to UBC use of the Zoom platform. The document will evolve through successive updates as required. These updates are reflected in the ”PIA Revision History” section, and details may be found under the Scope section of this document.

PART 1: GENERAL INFORMATION & OVERVIEW

1.4 Unit and Program Area

CAMPUS	UBC – all campuses
FACULTY OR DEPARTMENT	CTLT, UBC IT
PROGRAM AREA(S)	
ADDITIONAL INFORMATION	Part of the UBC unified response to the COVID-19 outbreak

1.2 Contact Information

NAME	Paul Hancock
TITLE / POSITION	Legal Counsel, Information and Privacy
FACULTY OR DEPARTMENT	Office of the University Counsel
UBC TELEPHONE NUMBER	604 822-2451
UBC E-MAIL ADDRESS	Paul.hancock@ubc.ca

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

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 UBC). 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 UBC IT will be focused on user administration, connectivity and support of users to be able to connect in to 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. Zoom and Skype for Business interaction may be made possible through the Pexip bridge with the 'Zoom Cloud Room Connector Add-On' feature.

UBC faculty will be directed to deliver on line classes via Zoom; a number of guidance documents have been created to assist staff and faculty in the delivery of classes via Zoom.

1.4 Scope of this PIA

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

As UBC has continued to review additional applications of the Zoom platform that may be leveraged to support the delivery of education and collaboration. Communication and change management requirements will continue to be the responsibility of the project team. As of August 30, 2020, the following additional uses have been reviewed and added to UBC's use of Zoom:

Mandatory Passcode

Beginning August 31st, 2020, UBC required all new Zoom meetings to have a passcode enabled for increased security. New meetings created as of August 31st will have a passcode automatically enabled and generated.

As part of this change, UBC is making the distinction of calling the codes that are unique to meetings "Passcodes" and will no longer be referring to them as "Passwords." Passcodes are meant to be shared with your invited meeting participants along with the meeting ID for access. "Passwords" will refer to users Zoom account login credentials.

Learning Tools Interoperability (LTI) Pro Canvas Integration

The Zoom LTI Pro Integration with Canvas is required to facilitate the use of Zoom from within the Canvas LMS creating a more seamless experience for faculty and students using Zoom for teaching and learning. It allows instructors to schedule and share synchronous lecture sessions with their students within Canvas without the need to distribute meeting links outside of Canvas thereby reducing the likelihood of "Zoom Bombing". The LTI Pro integration uses the primary email address in Canvas for the instructor to link with the instructor's Zoom account in order to schedule meetings. As such, the instructor's primary email address in Canvas must match the email address used to create their UBC Zoom account. The meetings are displayed to students enrolled in a Canvas section so that they can click a join button from within Canvas. (Note: Students who already have the Zoom client installed and associated with a Zoom account will automatically be logged in with that same Zoom account. If students wish to remain anonymous, they may wish to use the Zoom web client.) Instructors can also share web recordings of the course sessions with the students using the integration.

Breakout Rooms

Some faculty have identified a requirement for the use of pre-assigned breakout rooms, based on a pedagogical need. In order to use pre-assigned (or perpetual) break out rooms, the meeting host requires a list of the students' email addresses associated with their Zoom account. The host can then paste the email addresses into a spreadsheet template that Zoom provides, can the room assignments, and upload that file to Zoom. Because all UBC Zoom account holders are listed in the UBC Zoom directory, students in courses requiring the use of pre-assigned breakout rooms will be encouraged to sign up for UBC Zoom accounts with cwl@student.ubc.ca email (being rolled out for MS Teams currently) in order to anonymize themselves.

Exam Invigilation

As faculty may not be able to be in all Zoom sessions for invigilated exams on Zoom, some exams may be invigilated by Teaching Assistants. Faculty may record these sessions for academic integrity reasons. Such recordings may be made to the cloud with access to the recording only enabled for Teaching Assistants and Instructors. These recordings must be kept in accordance with UBC's retention policy for at least one year. They should be securely kept either in Zoom Cloud storage or should be transferred into UBC's enterprise video platform, Kaltura.

1.5 Related PIAs

A related PIA was completed by UBC's PrISM team in 2017 for use of Zoom as a fallback emergency communications channel for UBC's Incident Response Team. The scope of the use of Zoom and the PIA was limited to this specific business use of the Zoom services.

A related PIA was started (but not completed) in 2019 for the use of Zoom as a one-way video presentation channel for live-streaming of information and training sessions for the Integrated Renewal Program. Information requested to proceed with the PIA was not provided by the vendor. The IRP was authorized to proceed with use of Zoom subject to precautions to prevent the exchange of personal information or other sensitive information.

1.6 Elements of Information or Data Collected

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. UBC 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, user name, physical address, email address, phone numbers, and other similar identifiers	User name
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 unless cloud recording is turned on by the host. 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 user name, it is potentially reidentifiable through the mosaic effect.

*Recently Zoom issued an update to its iOS app which stops it sending certain data to Facebook. Previously, the 'Login with Facebook' feature notified Facebook when the user opened the app, provided details on the user's device such as the model, the time zone and city they are connecting from, which phone carrier they are using, and a unique advertiser identifier created by the user's device which companies can use to target a user with advertisements.[1] As far as the PIA team can determine, no such functionality exists in other operating systems.

Refer to APPENDIX A.01 for diagram and notes on data shared with other parties including for analytics.

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

This PIA is based on the configuration in which Zoom stores data in Canada. See section 2.1 for more information.

Regarding the LTI integration with Canvas, Zoom has advised the project team that all registration data is stored in the Canadian cluster. No data is stored in the US.

1.8 Data-Linking Initiative

This initiative in not considered a data linking initiative as contemplated in s.36.1 of FIPPA.

1.9 Is this a Common or Integrated Program or Activity? If so, how?

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

1.10 Risk Classification Level

The initial inherent risk classification level of this PIA submission at opening is VERY HIGH as determined by the Risk Classification Tool (RCT). The risk classification level of this PIA submission at closure is VERY HIGH.

[1] https://www.vice.com/en_us/article/z3b745/zoom-removes-code-that-sends-data-to-facebook

PART 2: PROTECTION OF PERSONAL INFORMATION

2.1 Personal Information Flow Diagram / Table

The following use case assumes that students are using the tool without opening an account. In this case, they only need to supply a login name to enter the meeting.

Personal Information Flow Table – Typical Learning Use Case

	Description/Purpose	Personal Information	Type	FIPPA Authority
1.	Instructor sends invitations to participate in Zoom session directly to students using CANVAS class lists 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 (Zoom Cloud recording) or in the user's local storage.	Discussion may include personal information of the speaker or of third parties.	Collection	26(c)
5.	Zoom administrators may monitor session, at UBC's request, in order to install, implement, maintain, repair, troubleshoot or upgrade the system. No data stored.	Login name and metadata.	Disclosure Inside Canada	33.2(a)

* this only applies if the student provides a login name that personally identifies them

Personal Information Flow Table – Zoom LTI Pro Integration

	Description/Purpose	Personal Information	Type	FIPPA Authority
1.	Instructor uses Zoom link in Canvas course to access meeting scheduling functionality. An LTI launch is performed in the background.	Instructor email addresses, Canvas Username, Canvas Display name	Use	32
2.	Student uses Zoom link in Canvas to access course meeting or view recorded course meetings. An LTI launch is performed in the	Student email addresses, Canvas Username, Canvas Display name	Collection	26(c)

	background however no personal information is stored by Zoom's servers.			
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 (Zoom Cloud recording) or in the user's local storage.	Discussion may include personal information of the speaker or of third parties.	Collection	26(c)
5.	Zoom administrators may monitor session, at UBC's request, in order to install, implement, maintain, repair, troubleshoot or upgrade the system. No data stored.	Login name and metadata	Disclosure Inside Canada	33.2(a)

	Personal Information Flow Table – Typical Administrative Use Case			
	Description/Purpose	**Personal Information**	**Type**	**FIPPA Authority**
1.	Employee sends invitations to participate in Zoom session directly to other employees at their UBC 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(a))
4.	If unrecorded, discussion flows through Zoom server without being stored there.	Discussion may include personal information of the speaker or of third parties.	Access within Canada	33.2(a)
5.	If recorded, discussion is stored on Zoom server (Zoom Cloud	Discussion may include personal information of the speaker or of third parties.	Collection, storage	26(c), 33.2(a)

	Personal Information Flow Table – Typical Administrative Use Case			
	Description/Purpose	**Personal Information**	**Type**	**FIPPA Authority**
	recording) or in the user's local storage.		within Canada	
6.	Zoom administrators may monitor session, at UBC's request, in order to install, implement, maintain, repair, troubleshoot or upgrade the system.	Metadata.	Access within Canada	33.2(a)

2.2 Risk Mitigation Table

Risk Mitigation Table				
	Risk	**Mitigation Strategy**	**Likelihood**	**Impact**
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.	Low	Low
2.	Non-compliance with FIPPA privacy notification requirement	All students receive a detailed privacy notification when they begin their studies at the university. Also, before each Zoom session, faculty members are required to advise them in writing of their options to maintain anonymity.	Low	Low
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.	Low	Low
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.	Medium	Low

Risk Mitigation Table				
	Risk	**Mitigation Strategy**	**Likelihood**	**Impact**
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 UBC administrators will ensure that identified vulnerabilities have been patched. Also, if users follow UBC guidance to turn off the record feature, no sensitive personal information will be collected and stored.	Low	High
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.	Low	Low
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.	High	Low
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.	Low	Low
9.	Faculty or staff may not have appropriate security controls in place if they are delivering classes while working remotely	UBC has guidance in place for remote working - http://www.hr.ubc.ca/faculty-staff-resources/telecommuting/	Low	Low
10.	Vendor may change terms of use of the service	UBC will negotiate terms in its enterprise license to address this. In the meantime, UBC will monitor the terms of use for changes.	Low	Low
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	High	Low

Risk Mitigation Table				
	Risk	Mitigation Strategy	Likelihood	Impact
		using privacy browser extensions to prevent third-party trackers from accessing their information.		

2.3 Collection Notice

All students are given a standard personal information collection notice when they apply for entry to UBC. 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 Privacy Matters (PrISM) team if necessary.

2.4 Disclosure of Student Information

As student information may be disclosed to other students, instructors should inform students in writing that, "The name you use to log into this system will be shared with other students. To protect your privacy, when you sign in you may provide your first name or a false name, and you may disable the audio and video; also, don't share any personal information during the session unless you are comfortable doing so."

If, alternatively, students decide to use their real names to identify themselves, then the metadata stored on the Zoom server about their use of the site will be personally identifying. It is important to keep in mind that while Zoom does disclose metadata to third parties for advertising purposes, as described above, it does not disclose the user name to these third parties.

The above process does not give the students a choice about whether to use Zoom, because all students need to use the same tool to access the meeting. However, the process ensures that students understand their options to anonymize themselves and reminds them about other precautions they can take to protect their privacy. The process should be part of a larger process of student education about how to protect their privacy when using cloud-based tools.

2.5 Exam Invigilation

Use for Exam Invigilation Purposes: Zoom may be used for exam invigilation purposes. This requires students to turn on their webcam during the exam. At the start of the exam, students would have to hold their IDs up to the webcam for verification of their identity. At any point during the exam, students could be asked to share their screen with the invigilator, to be certain they are not looking at prohibited materials. Due to the sensitivity of the information provided during this process, recording must be disabled.

Updated: Exam Invigilation

As noted in the "Updated Scope" section of this assessment, some exams may be invigilated by Instructors and Teaching Assistants. Faculty may request to record these sessions for academic integrity reasons. To support this need, recordings may be made to the Zoom cloud with access to the recording only enabled for Teaching Assistants and Instructors. This access will be approved by individual Deans' offices. In keeping with UBC policies on final exams, the recordings will be retained for one year plus a day.

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

Consent is not required as Zoom stores all UBC personal information within Canada.

PART 3: SECURITY OF PERSONAL INFORMATION

3.1 Physical Security Measures

UBC requires data centres to comply with a detailed set of security requirements.[2] The Zoom application is hosted on external cloud-based commercial infrastructure sites. Zoom is hosted within AWS (Amazon Web Services) in Canada. The physical security capabilities of AWS data centres meet or exceed the UBC standard.

3.2 Technical Security Measures

UBC has several information security standards that set out the minimum requirements for the protection of sensitive data.[3]

Under its Privacy Policy[4] web-page Zoom states:

> **Security of your Personal Data**
> Zoom is committed to protecting the Personal Data you share with us. We utilize a combination of industry-standard security technologies, procedures, and organizational measures to help protect your Personal Data from unauthorized access, use, or disclosure. When we transfer credit card information over the Internet, we protect it using Transport Layer Security (TLS) encryption technology.

Zoom also states that it[5]:

- Submits privacy practices to independent assessment and certification with Trust Arc
- Undergoes an annual SSAE-16 SOC 2 audit by a qualified independent third-party
- Performs regular vulnerability scans and penetration tests to identify new threats
- Executes “Data Protection Agreements” for adequate transfer mechanisms
- Protects data in transit by TLS 1.2 using 256-bit Advanced Encryption (AES-256)
- Leverages the physical and environmental protection of our TIER 1 data center providers. Zoom’s hosting facilities have 24/7 manned security and monitoring
- Does not monitor, view, or track the video or audio content of meetings or webinars
- Does not share customer data with third parties
- Limits retainment of accounts to 30 days after termination to assist with product reactivation upon request. After 30 days, the account is permanently deleted

Zoom has provided additional security information to UBC subject to an NDA.

The PIA team has also collected information from third parties on this subject. Refer to APPENDIX A.01 for additional information which was obtained from an external entity PIA. UBC has also

[2] Information Security Standard #18, Physical Security of UBC Datacentres https://cio.ubc.ca/sites/cio.ubc.ca/files/documents/standards/Std%2018%20Physical%20Security%20of%20UBC%20Data%20Centres.pdf

[3] https://cio.ubc.ca/information-security/information-security-policy-standards-and-resources#management_standards

[4] https://zoom.us/privacy/

[5] https://blog.zoom.us/wordpress/2018/11/12/zoom-serves-canadian-healthcare-pipeda-phipa-compliance/

reviewed the reports of two significant security issues that Zoom has experienced during the last two years:

- In November 2018, a security vulnerability (CVE-2018-15715) was discovered which allowed a remote unauthenticated attacker to spoof messages from a meeting attendee or Zoom server in order to invoke functionality in the target client. This would allow the attacker to remove attendees from meetings, spoof messages from users, or hijack shared screens.

- In July 2019, security researchers disclosed a vulnerability which allowed any website to forcibly join a macOS user to a Zoom call, with their video camera activated, without the user's permission. In addition, attempts to uninstall the Zoom client on macOS would prompt the software to re-install automatically in the background, using a hidden web server that was set up on the machine during the first installation and that remained active even after attempting to remove the client. After receiving public criticism, Zoom updated their software to remove the vulnerability and the hidden webserver, allowing for complete uninstallation.

Without intending to minimize the seriousness of the above security issues, the PIA team does not believe that they represent a systemic problem with Zoom's technical security measures. Based on the information reviewed, the PIA team has concluded that the Zoom system complies with UBC's Information Security Standards and has adequate technical security measures in place for the purposes contemplated by UBC.

3.3 Security Policies, Procedures, and Standards

N/A

3.4 Tracking Access / Access Controls

N/A

PART 4: ACCURACY, CORRECTION, AND RETENTION

4.1 Updating and Correcting Personal Information

UBC 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.

4.2 Decisions That Directly Affect an Individual

Zoom will not be used to record any information that is used to make a decision that affects any individual. Recording of personal information is not permitted.

4.3 Records Retention and Disposal

Unfortunately, Zoom is not capable of automatically applying retention schedules to the information it collects. Zoom does not allow recorded information to be deleted until the account has been deleted. Program design reduces this risk through limiting the sensitivity of recorded information. See discussion in Summary and Recommendations section.

PART 5: FURTHER INFORMATION

5.1 Systematic Disclosures of Personal Information

This initiative does not involve the systematic disclosure of personal information.

5.2 Access for Research or Statistical Purposes

This initiative does not involve disclosure of personal information for research purposes.

5.3 Other Applicable Legislation

N/A

5.4 Other

N/A

PART 6: ACCESS AND PRIVACY MANAGER COMMENTS

6.1 Conclusions and Conditions

Overall Conclusion
This Privacy Impact Assessment has determined that, provided the condition listed below are implemented, the services in scope can be delivered in compliance with FIPPA and UBC policies. Should the scope of the program change, further assessments may be required as new related or expanded services are considered, and through post implementation to ensure the programs delivered match those proposed.

From a privacy and security perspective, it is important to distinguish between learning and administrative use cases.

Learning use cases generally collect very little personal information. The typical learning session is a lecture to a large class (in the order of hundreds of students) with little or no opportunity for students to interact with the instructor. In these sessions, the only personal information that is collected and stored on the Zoom servers is the names of users, and associated metadata about their use of the site. This is relatively low risk information. Moreover, it is unlikely that sensitive personal information will be shared in the teaching session. For this reason, we recommend that UBC should allow instructors to record learning sessions provided they comply with all other required conditions.

Administrative use cases are much more difficult to generalize, as they may or may not collect sensitive personal information. UBC should therefore discourage recording of all administrative meetings, and prohibit recording of any sessions in which personal information is likely to be discussed.

Updated Conclusions and Conditions
As described in the Introduction section of this document, the Assessment is an evergreen document and will be updated as new uses of the Zoom platform are added. Any additional risks and related conditions reviewed and documented in this Assessment are limited to the Learning use cases.

Conditions Relating to Learning Use Cases

Condition #1: Remind Faculty Members to use Faculty Self Service Centre to Send Zoom Invitations to Students
UBC should advise faculty members to send email invitations to students to participate in Zoom meetings using the Faculty Self Service Centre. This eliminates the risk of students seeing each other’s email addresses.

Condition #2: Allow Students to Anonymize Themselves in Classes

As student information may be disclosed to other students, instructors should inform students in writing that, “The name you use to log into this system will be shared with other students. To protect your privacy, when you sign in you may provide your first name or a false name, and you may disable the audio and video; also, don't share any personal information during the session unless you are comfortable doing so."

Condition #3: Educate Students about Metadata Disclosure to Third Parties

As far as we can determine, the only information Zoom makes available to third-party service providers and advertising partners various non-identifying metadata about the use of the site. This metadata, which is collected by cookies and similar technologies, includes Internet protocol (IP) addresses, browser type, Internet service provider (ISP), referrer URL, exit pages, the files viewed on our site (e.g., HTML pages, graphics, etc.), operating system, date/time stamp, and/or clickstream data. Zoom states that the purpose of this disclosure is "to offer and improve our services, trouble shoot, and to improve our marketing efforts." For example, metadata may be used by Google to drive targeted advertising. Zoom has assured UBC that user names are not provided to advertising partners. There is, of course, a risk that third parties will be able to identify the user by linking that data to other available data in their possession.

It is commonplace for websites to track access to their sites for targeted advertising purposes. While this widespread practice has privacy implications, the PIA team does not believe that this practice, on its own, should stop UBC from using Zoom. However, the PIA Team recommends that UBC support additional efforts to educate students about cloud privacy practices, such as using privacy browser extensions such as Privacy Badger to prevent third-party trackers from accessing your information. We note that UBC already has some excellent resources available to students on digital privacy, such as the Digital Tattoo project: https://digitaltattoo.ubc.ca/tutorials/privacy-and-surveillance/online-presence/.

Conditions Relating to Administrative Use Cases

Condition #4: Limit Recording in Administrative Use Cases

In administrative use cases, UBC must provide guidance for faculty and staff that it is acceptable for them to use Zoom on the following conditions:

- If meeting hosts are inviting non-employees to participate in a meeting, the host must inform these participants that the name they use to log in to the system will be shared with other participants and they can protect their privacy as follows:

(i) use a first name or a substitute name rather than their full name,

(ii) turn off their audio and video, and

(iii) not disclose any personal information during the session (unless that is the purpose of the meeting).

- If the purpose of the meeting is to discuss personal information, the meeting must not be recorded. This reduces the risk of inadvertent access or disclosure of personal information.

Technical Conditions

Condition #5: Apply Settings to Selected Zoom Features

The PIA team has analyzed Zoom features using a privacy and security lens. A list of the identified features and the required settings is contained in Appendix B.

6.2 Summary of Conditions of Approval

#1: Remind Faculty Members to use Faculty Self Service Centre to Send Zoom Invitations to Students

#2: Allow Anonymization in Learning Use Cases

#3: Educate Students about Metadata Disclosure to Third Parties

#4: Limit Recording in Administrative Use Cases

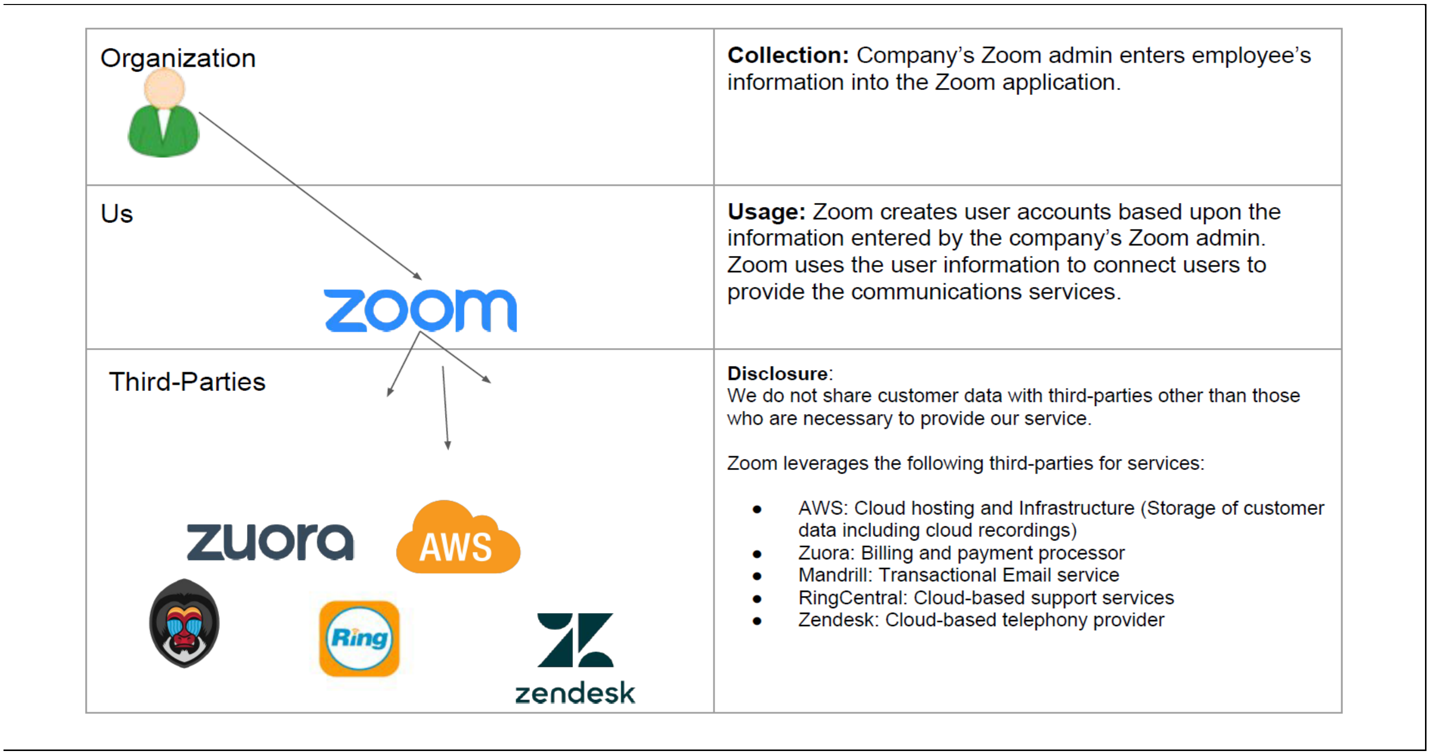
#5: Apply Settings to Selected Zoom Features

APPENDIX A

A.01 Information Flow Schematic

The following high-level schematic was obtained from a PIA document prepared for the Educational Resources Acquisition Consortium (ERAC), a cooperative member-based BC organization.

The ERAC document states the following diagram was provided by Zoom. However, the diagram's authenticity and source have not been verified. It is noted that the diagram "makes sense" based on information provided in another Zoom documentation and webpage content.



Organization	**Collection:** Company's Zoom admin enters employee's information into the Zoom application.
Us	**Usage:** Zoom creates user accounts based upon the information entered by the company's Zoom admin. Zoom uses the user information to connect users to provide the communications services.
Third-Parties	**Disclosure**: We do not share customer data with third-parties other than those who are necessary to provide our service. Zoom leverages the following third-parties for services: • AWS: Cloud hosting and Infrastructure (Storage of customer data including cloud recordings) • Zuora: Billing and payment processor • Mandrill: Transactional Email service • RingCentral: Cloud-based support services • Zendesk: Cloud-based telephony provider

The above diagram was accompanied by the following text excerpt, which appears to have ben copied from the Zoom online documentation:

> Zoom is a Software as a Service (SaaS) offering that uses Amazon Web Services (AWS) infrastructure for hosting. Designated administrators enter information into the Zoom App which talks to AWS Relational Database service (RDS). If information matches, AWS RDS establishes meeting connection.

The following additional information was also included regarding the sub-processors listed in the diagram.

<u>Sub-processors</u>

Zoom uses certain Sub-processors to support delivery of their services (listed below). A sub-processor is a third-party data processor engaged by Zoom, who has or potentially will have access to or process customer data.

Prior to engaging any third part sub-processor, Zoom has evaluated their security and privacy standards.

Sub-processor Identity	Sub-processing Activities	Location
Amazon Web Services	Cloud Service Provider	Canada
Zuora	Billing and payment processing	United States
Zendesk	Cloud-based customer support services	United States
Mandrill	Cloud-based transactional email services	United States
Ring Central	Cloud-based telephony provider	United States

APPENDIX B

Required Settings for Selected Zoom Features

Category	Description	Locked Setting (Cannot be Changed by Meeting Host)	Default Setting (Can be Changed by Meeting Host)
Scheduling the Meeting	**Host video -** Start meetings with host video on		OFF
	Participants video - Start meetings with participant video on. Participants can change this during the meeting.		OFF
	Join before host - Allow participants to join the meeting before the host arrives		OFF
	Use Personal Meeting ID (PMI) when scheduling a meeting, when starting an instant meeting, and when starting an instant meeting. Your PMI is essentially one continuous meeting and people can pop in and out all the time.		OFF
	Only authenticated users can join meetings - The participants need to authenticate prior to joining the meetings, hosts can choose one of the authentication methods when scheduling a meeting. Default option is 'Sign in to Zoom'.		OFF
	Require a password when scheduling new meeting - A password will be generated when scheduling a meeting and participants require the password to join the meeting. The Personal Meeting ID (PMI) meetings are not included.		On
	Embed password in meeting link for one-click join - Meeting password will be encrypted and included in the join meeting link to allow participants to join with just one click without having to enter the password.		ON
	Mute participants upon entry - Automatically mute all participants when they join the meeting. The host controls whether participants can unmute themselves.		ON
In the Meeting (Basic)	**Require Encryption for 3rd Party Endpoints (H323/SIP)** - Zoom requires encryption for all data between the Zoom cloud, Zoom client, and Zoom Room. Require encryption for 3rd party endpoints (H323/SIP).	ON	
	Chat - Allow meeting participants to send a message visible to all participants.		ON
	Prevent participants from saving chat		OFF
	Auto saving chats - Automatically save all in-meeting chats so that hosts do not need to manually save the text of the chat after the meeting starts.		OFF
	File transfer - Hosts and participants can send files through the in-meeting chat.		OFF
	Feedback to Zoom - Add a Feedback tab to the Windows Settings or Mac Preferences dialog, and also enable users to provide feedback to Zoom at the end of the meeting		ON
	Disable desktop/screen share for users - Disable desktop or screen share in a meeting and only allow sharing of selected applications.		OFF
	Remote control - During screen sharing, the person who is sharing can allow others to control the shared content		ON

In Meeting (Advanced)	**Far end camera control -** Allow another user to take control of your camera during a meeting		OFF
	Virtual background - Allow users to replace their background with any selected image. Choose or upload an image in the Zoom Desktop application settings.		ON
	Identify guest participants in the meeting/webinar - Participants who belong to your account can see that a guest (someone who does not belong to your account) is participating in the meeting/webinar. The Participants list indicates which attendees are guests. The guests themselves do not see that they are listed as guests.		ON
	Attention tracking - Lets the host see an indicator in the participant panel if a meeting/webinar attendee does not have Zoom in focus during screen sharing.	OFF	
	Waiting room - Attendees cannot join a meeting until a host admits them individually from the waiting room. If Waiting room is enabled, the option for attendees to join the meeting before the host arrives is automatically disabled.		OFF
	Blur snapshot on iOS task switcher - Enable this option to hide potentially sensitive information from the snapshot of the Zoom main window. This snapshot display as the preview screen in the iOS tasks switcher when multiple apps are open.		ON
	Show a "Join from your browser" link - Allow participants to bypass the Zoom application download process, and join a meeting directly from their browser. This is a workaround for participants who are unable to download, install, or run applications. Note that the meeting experience from the browser is limited		OFF
	Phone - Mask phone number in the participant list - Phone numbers of users dialing into a meeting will be masked in the participant list. For example: 888****666		ON
Recording	**Local recording -** Allow hosts and participants to record the meeting to a local file.		ON
	Hosts can give participants the permission to record locally		ON
	Cloud recording - Allow hosts to record and save the meeting / webinar in the cloud. *Note: Advanced options allow the host to record PI, e.g. participant names and images, chat messages.*	ON	
	Automatic recording - Record meetings automatically as they start		OFF
	Require password to access shared cloud recordings - Password protection will be enforced for shared cloud recordings. A random password will be generated which can be modified by the users. This setting is applicable for newly generated recordings only		OFF
	Auto delete cloud recordings after days - Allow Zoom to automatically delete recordings after a specified number of days		OFF
	Recording disclaimer - Show a customizable disclaimer to participants before a recording starts.		OFF
	Multiple audio notifications of recorded meeting - Play notification messages to participants who join the meeting audio. These messages play each time the recording starts or restarts, informing participants that the meeting is being recorded.		ON