



OFFICE OF THE VICE-PRESIDENT, LEGAL AFFAIRS
Archives and Records Management Department

PRIVACY IMPACT ASSESSMENT
for
Zoom Videoconferencing Platform

1. Purpose of the Privacy Impact Assessment (PIA)

This form is used by SFU to determine if a current or proposed policy, system, project, program or activity meets or will meet the protection of privacy requirements under Part 3 of the British Columbia *Freedom of Information and Protection of Privacy Act* (FIPPA). The Act makes it a legal requirement that SFU conduct a PIA in accordance with the directions of the minister responsible for the Act. The PIA is a risk management and compliance tool to identify potential privacy issues and impacts, allowing correction and mitigation, thus avoiding costly system, program, service, or process redesign; privacy complaints or breaches; and harm to personal, professional and institutional reputation.

See Schedule A for definition of terms.

Archives and Records Management Department use only			
Office of primary responsibility	IT Services	Approved date	October 19, 2020
PIA #	2020-004	OIPC notified date	
Type of PIA	☐ Department ☒ Corporate ☐ Update	OIPC response date	
Type of PIA review	☐ Policy ☒ System	☐ Project	
(Check all that apply)	☐ Program ☐ Activity		
Other applicable PIA provisions	☐ Common or integrated program	☐ Data-linking initiative	
(Check all that apply)	☐ Information sharing agreement		

2. General Information

2.1. Unit and Program Area

Identify the Department and Program submitting this PIA

Department:	IT Services
Program:	SFU Zoom Implementation

2.2. Contact

Identify the individuals best positioned to speak to the contents of this PIA

Name of PIA Drafter:	Melissa Luck		
Position Title:	Project Manager		
Phone:	2-2246	E-Mail:	mluck@sfu.ca
Name of Program Manager:	Mark Jutras		
Position Title:	Service Owner, Videoconferencing		
Phone:		E-Mail:	mjutras@sfu.ca

2.3. Description of the Current or Proposed Policy, System, Project or Program

Provide as background a general description of the initiative and the context in which it functions. This could include the purpose of the initiative and its benefits, what larger process it is part of, how it functions, how it integrates with or consolidates other information systems, how it aggregates and stores together information that was previously maintained separately, how it converges different record keeping systems, the parties involved, how it will automate or otherwise change the existing business workflow, etc. Describe in the sections immediately following the background (if applicable) specific details with respect to the individual actors involved in the business process, focusing on how their personal information will be collected, accessed, used, disclosed and retained.

Include copies of documentation (if it exists) that describe the business requirements, functional analysis, conceptual overview, etc. that helps explain the initiative.

2.3.1. Background

Project Overview

In mid-March, a pilot implementation of Zoom – a videoconferencing platform – was initiated as part of SFU's COVID-19 response to supporting remote work, teaching, learning, and research. Zoom has grown to be the market leader in videoconferencing due to its ease of use, reliability, and availability of free accounts to the general public (with a limited feature set). Consequently, SFU has seen a rapid rise in demand from the faculty, staff, and student community as an alternative or additional option to existing services

such as BlueJeans, Mediasite, and Blackboard Collaborate Ultra. Zoom is already in use by many other Canadian higher education institutions. Although retirees, Alumni, and former faculty/staff/students are not eligible to obtain user accounts, they will still be able to participate in Zoom meetings as attendees, as will any non-SFU (external) individual.

Data Centers and Hosting

Zoom 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 in the United States and around the world. In SFU's configuration, data provided by users is stored in US servers. Data in transit will either be through Canadian or US-based servers: This is dependent on the participant's location and the nearest data centre.

Integration with Single Sign-On (SSO)

SFU's deployment of Zoom will provide user accounts to all faculty, staff, and students for self-service creation and management of Zoom meetings. Sponsored accounts paid for by administrative or academic departments/faculties at SFU are also eligible to obtain Zoom accounts; they cover use cases such as roles (e.g., itsinfo@sfu.ca), sessional instructors, and temporary staff. Role accounts are typically used by SFU faculty, staff, or students and often act as their preferred primary account for day-to-day responsibilities. One-way integration with SFU's Central Authentication Service (CAS) that features single sign-on (SSO) via Shibboleth is currently in place, passing a limited set of data elements in the account creation process as described in subsequent sections of this document. No other sign-in methods (e.g., Facebook or Google) will be offered.

While SFU is providing licensed Zoom accounts to faculty, staff, and students with login through SSO, it is possible that the same individuals would have access to a separate personal Zoom account (i.e., a free account) or a licensed account through other means. An individual may be using their non-SFU Zoom account, either intentionally or unintentionally, to perform teaching, learning, work, and/or research-related activities without SFU's knowledge. One such scenario would be someone using a free account to record a meeting (SFU's enterprise license has recording enabled only for faculty and staff).

User Types and Roles

There are several user types, applicable to Zoom meetings and Zoom webinars:

- **SFU enterprise account user:** An SFU faculty member, staff member, sponsored account user, or student using a Zoom account licensed under SFU's enterprise agreement using integration with SSO for a one-time import of a limited set of data elements (first name, display name, last name, SFU email address, and department).
- **Non-SFU account user:** An SFU community member (can be faculty, staff, sponsored account user, student, Alumni, retiree, individuals with former faculty/staff/student roles, etc.) using a Zoom account licensed outside of SFU's enterprise agreement. Possible scenarios include personal purchase of a license, a license provided by an individual department/unit/faculty at SFU, or a license provided by an institution/company outside of SFU. For those eligible for an SFU enterprise account (i.e., current faculty, staff, students, sponsored accounts) who had their non-SFU account created using their SFU email address, they will be

presented with the option of converting to an SFU enterprise license account at any time.

- **Free account user:** An SFU community member (can be faculty, staff, sponsored account user, student, Alumni, retiree, individuals with former faculty/staff/student roles, etc.) using the no-cost version of a Zoom account. Normally associated with a non-SFU email address. Any free account user who had created their account using their SFU email address will have three logins to decide whether they want to convert their account to an SFU enterprise license account, or change the associated email address to a non-SFU address.
- **Non-account user:** An SFU community member (can be faculty, staff, student, Alumni, retiree, individuals with former faculty/staff/student roles, etc.) participating as an attendee without the usage of a Zoom account, i.e., through the web client. The web client allows non-account users to specify any username, identifying or non-identifying, to offer the option of preserving anonymity. However, this presents challenges in allowing a meeting host to verify attendees' identities for use cases such as class participation evaluation. IT Services will soon require all users use Enterprise version; however, uncertain if external users or non-enterprise versions can join or what are the additional risks. This requirement and the possible risks of participation by non-enterprise users will be updated and advertised on the SFU ITS website as developed.

For Zoom meetings, the following roles exist:

- **Host:** Creates, manages, organizes the meeting using their Zoom account. Once a meeting has started, a host can assign a co-host with the ability to change settings, mute/unmute attendees, and add/remove attendees (i.e., a subset of what a host is able to do). Hosts/co-hosts can be SFU enterprise account users, non-SFU account users, or free account users.
- **Attendee:** Attends and participates (audio/video discussion, chats, screen sharing) in a Zoom meeting through their Zoom account, with the option of using the Zoom web app, desktop app, or mobile app. Attendees can be of any user type, i.e., SFU enterprise account user, non-SFU account user, free account user, or non-account user.

For Zoom webinars, the following roles exist:

- **Host:** Creates, manages, organizes the webinar using their Zoom account. Once a webinar has started, a host can assign a co-host with the ability to change settings, mute/unmute attendees, add/remove attendees, and promote/demote panelists attendees (i.e., a subset of what a host is able to do). Hosts/co-hosts can be SFU enterprise account users or non-SFU account users.
- **Panelist:** Is the primary presenter(s) in a webinar with the ability to share content. Panelists can be SFU enterprise account users, non-SFU account users, or free account users.
- **Attendee:** Attends and participates in a Zoom webinar through their Zoom account, with the option of using the Zoom web app, desktop app, or mobile app. Attendees can be of any user type, i.e., SFU enterprise account user, non-SFU account user, free account user, or non-account user.

Product Usage

A Zoom meeting refers to a video conferencing meeting that is hosted by an individual using Zoom, with a meeting capacity of up to 300 attendees. When an attendee joins a Zoom meeting, they are given the option to turn on their webcam or microphone (video

and audio for attendees is muted by default). Aside from recording within Zoom, meetings can potentially be recorded by the meeting host or any of its attendees using a third-party application. Meetings can be hosted and attended from a desktop application (Windows and Mac OS), web application, or mobile application (Android and iOS). SFU has disabled the option of syncing Exchange calendar and contacts with Zoom as it requires the user to enter their SFU Computing ID and password to establish the sync with SFU Mail. Virtual backgrounds (i.e., custom backgrounds that hide the actual background) can be used by the host and each attendee, though it is known that some devices may not have the appropriate technical specifications to support this functionality, resulting in no ability to hide a personal environment aside from turning video off.

The majority of Zoom's mobile apps' features are the same as those available on the desktop app. Notable features with potential privacy/security impacts that are *unavailable* on the mobile apps are as follows:

- starting a local recording session,
- creating, editing, or launching polls,
- controlling who can share their screen in the meeting,
- pausing your current shared screen,
- manually change your status (Available, Away, or Do Not Disturb),
- editing sent chat messages,
- sending a capture of the current screen, animated GIFs, or code snippets in chat,
- managing blocked contacts, and
- using a virtual background (available on iOS but not for Android).

SFU has also purchased Zoom's webinar product, licensed separately, that provides the capability of hosting presentations to large-scale audiences of up to 500 attendees with up to 100 concurrent presenters, i.e., "panelists" including a host/co-host(s). Only panelists and hosts have the ability to share video and audio content while attendees have view-only access. Attendees can be "promoted" to become panelists by the webinar host, co-host(s), or Zoom Admins, and panelists can be "demoted" to become attendees in the same manner. This product is suited to accommodate use cases such as large lectures, town hall events, and public events (SFU Public Square, etc.).

Assumptions

The following is a list of assumptions considered in the development of this PIA:

- Zoom is the only tool under consideration that is capable of multi-way-interaction videoconferencing sessions that can accommodate up to 300 attendees per session.
- SFU is planning to use Zoom for remote teaching, learning, and research 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.
- Zoom employees will not actively monitor any customer sessions unless SFU requests them to do so for support or troubleshooting purposes.
- Due to its surge in popularity in recent months, Zoom will continue to respond and action on privacy and security-related concerns at an accelerated pace, resulting in more frequent changes to the product and/or its services.

- SFU will adjust administrative configuration and settings in response to changes to feedback from the SFU community and/or changes in Zoom's product and/or services, as described above.

2.3.2. SFU Enterprise Account Users

Collection: Information from SFU enterprise account users will be auto-populated via SFU Shibboleth, obtained by manual entry by the user, and through logs in the case of usage information, device information, and metadata.

Depending on usage including whether the user is an account owner or only an attendee, data elements may include:

- Identifiers: First name, display name, last name, SFU email address, physical address, phone number, approximate location
- Employment information: job title, company
- User preferences: Configuration such as enabling waiting room, muting audio/video for participants upon entry, etc.
- Device and network information: e.g., IP address, MAC address, device type, operating system
- Usage information: a log of activities including switching between desktop/mobile clients, type of phone used, etc.
- Meeting metadata: subject, description, participants, meeting statistics/metrics, join/leave time.
- User generated content: chats, video, audio, polls, screen shares, annotations, and whiteboard diagrams.

Access: Zoom Support and SFU's Zoom Administrators will have the access to all of the data elements listed above. SFU's Zoom Administrators will have the ability to set default configuration as well as lock settings to prevent manual override by users. As an account owner, a user is able to access account settings/configuration, their user profile, and data associated with scheduling meetings. As an attendee, they will be able to access their own meeting settings/preferences.

Use: Zoom Support and SFU's Zoom Administrators will be using the above data elements for troubleshooting and support purposes. Examples include investigation of connectivity issues and unexpected behavior in the web, desktop, or mobile apps. As an account owner, the data will be used to confirm their preferences in the setup of their account and meetings. Attendees will be using personal information for identification and collaboration purposes.

Disclosure: The personal information outlined above will be viewable by Zoom Support and SFU's Zoom Administrators. Zoom account owners will be able to view their profile information, settings, and a limited set of activity pertaining to meetings. Attendees will be able to view a user's username, other profile-related details as entered by the user as the account owner.

Retention: Zoom will accommodate specific requests for deleting information. By default, chat transcripts must be manually saved by the user and are otherwise deleted once the session has ended.

2.3.3. Non-SFU Account Users and Free Account Users

SFU Zoom Administrators have no control over the configuration and default user settings of Non-SFU and Free Accounts – this is done by Zoom Support, or local administrators in the case of the non-SFU set of licenses. Collection, access, use, disclosure, and retention of personal information will differ from SFU's enterprise license accounts as a result.

Collection: Information from SFU enterprise account users will be obtained by manual entry by the user, and through logs in the case of usage information, device information, and metadata.

Depending on usage including whether the user is an account owner or only an attendee, data elements may include:

- Identifiers: First name, display name, last name, SFU email address, profile image, physical address, phone number, approximate location
- Employment information: job title, company
- User preferences: Configuration such as enabling waiting room, muting audio/video for participants upon entry, etc.
- Device and network information: e.g., IP address, MAC address, device type, operating system
- Usage information: a log of activities including switching between desktop/mobile clients, type of phone used, etc.
- Meeting metadata: subject, description, participants, meeting statistics/metrics, join/leave time.
- User generated content: chats, video, audio, polls, screen shares, annotations, and whiteboard diagrams.
- SFU credentials (i.e., SFU Computing ID and password) for calendar and contacts sync, if enabled by the administrator(s).

Access: Zoom Support and local administrators of the non-SFU accounts will have access to all of the data elements listed above. Local administrators will have the ability to set default configuration as well as lock settings to prevent manual override by users. As an account owner, a user is able to access account settings/configuration, their user profile, and data associated with scheduling meetings. As an attendee, they will be able to access their own meeting settings/preferences.

Use: Zoom Support and local administrators will be able to use the above data elements for troubleshooting and support purposes. Examples include investigation of connectivity issues and unexpected behavior in the web, desktop, or mobile apps. As an account owner, the data will be used to confirm their preferences in the setup of their account and meetings. Attendees will be using personal information for identification and collaboration purposes.

Disclosure: The personal information outlined above will be viewable by Zoom Support and local administrators. Zoom account owners will be able to view their profile information, settings, and a limited set of activity pertaining to meetings. Attendees will be able to view a user's username, other profile-related details as entered by the user as the account owner.

Retention: Zoom will accommodate specific requests for deleting information.

2.3.4. Non-Account Users (i.e., Attendee Only)

Collection: Information from this group of users is obtained by manual entry by the user, and through logs in the case of usage information, device information, and metadata.

Members of this user group can only participate as attendees. Data elements may include:

- Identifiers: Username, email address, phone number, approximate location
- Device and network information: e.g., IP address, MAC address, device type, operating system
- Usage information: a log of activities including switching between desktop/mobile clients, type of phone used, etc.
- Meeting metadata: e.g., participants, join/leave time, etc.
- User generated content: chats, video, audio, polls, screen shares, annotations, and whiteboard diagrams.

Access: Zoom Support and SFU’s Zoom Administrators or local administrators (depending on the user type of the host) will have access to activity logs and the ability to set default configuration as well as lock settings to prevent manual override by users. As attendees, members of this user group will be able to access their own meeting settings/preferences while the session is active.

Use: Zoom Support and SFU’s Zoom Administrators or local administrators will be able to use this information for troubleshooting and support purposes. Examples include investigation of connectivity issues or unexpected behavior in the web application. Attendees and the meeting organizer will be using this information for identification and collaboration purposes.

Disclosure: The majority of the information will be viewable by Zoom Support and SFU’s Zoom Administrators or local administrators. Non-account users will be able to view their profile information, settings, and a limited set of activity pertaining to meetings. Attendees will be able to view the username, other profile-related details as entered by the user as an attendee.

Retention: Zoom will accommodate specific requests for deleting information.

2.4. Scope of this PIA

Explain exactly what the PIA covers and conversely what it does not.

This PIA covers the usage of the Zoom videoconferencing platform by faculty, staff, and students at SFU for the purposes of remote work, teaching, learning, and research. The details of this PIA apply to SFU's specific configuration of Zoom.

The following functions within the Zoom platform will be covered:

- Zoom meetings, including the chat functionality within meetings,
- Zoom’s web, desktop, and mobile applications, and
- Zoom webinars.

Depending on the refinement of the project’s scope, future amendments to this PIA may cover select apps and plugins (e.g., Outlook).

This PIA does not cover:

- Instant messaging (IM) functionality. This will be deactivated in SFU's implementation of Zoom,
- Zoom Rooms, i.e., configuration of physical meetings rooms fitted with audio and visual equipment integrated with the Zoom platform,
- Other apps and plugins deemed out of scope of the project,
- Zoom Phone, i.e., Zoom's cloud-based phone system, and
- Non-SFU enterprise Zoom licences that may be held by SFU departments and community members

2.5. Related PIAs

Identify PIAs for other parts of the initiative or any PIAs that were previously completed for this initiative.

None identified.

2.6. Elements of Information or Data

List the types of personal information involved in the initiative (if applicable). This could include the individual's name, age, address, work/home email, work/home phone number, educational history, employment history, work status, health information, financial information, photos, comments, or opinions about third parties. See Schedule A for a partial list of types of personal information.

2.6.1. SFU Enterprise Account Holders

Category	Collection	Access	Use	Disclosure
Identifiers	Auto-populated via SFU Shibboleth at Zoom account creation: • First name • Display name • Last name • SFU email address Via user entry at Zoom account setup: • Physical address • Phone number • Approximate location	• Zoom Support through admin tools • SFU Zoom Admin through admin tools • Account Owner through self-service account management interface • Attendees via participation in a session	• Create a user account • Communicate with a user • Respond to requests for support • Viewing a user's profile for identification and/or contact information	• Display name, is viewable when attendees hover over your profile in desktop client. • Display name viewable by attendees in Zoom meetings via attendee list.
Employment information	Via user entry at Zoom account setup: • Job title • Company	• Zoom Support through admin tools	• Create a user account • Viewing a user's profile for	None

Category	Collection	Access	Use	Disclosure
		- SFU Zoom Admin through admin tools - Account Owner through self-service account management interface	identification and/or contact information	
User preferences	Via user entry at Zoom account setup; Service preferences and configuration such as enabling a waiting room, muting video/audio for attendees, etc.	- Zoom Support through admin tools - SFU Zoom Admin through admin tools - Account Owner through self-service account management interface	To provide user with choices for how to use/configure Zoom	None
Device and network information	Via Zoom meeting participation: Information on a user's device, network, and internet connection, such as: - IP address(es) - MAC address - Other device ID (UDID) - Device type - Operating system type and version - Client version	- Zoom Support through admin tools and logs - SFU Zoom Admins through admin tools and logs	- Provide dashboards and reports - Respond to requests for support - Monitor performance of data centers and networks - Conduct anonymized, aggregated analytics to improve Zoom's service performance	None
Usage information	Via Zoom meeting participation: Usage activities and other interaction with the service, such as whether a user switched between mobile client to desktop client, whether a user used VoIP or phone call, etc.	- Zoom Support through admin tools and logs - SFU Zoom Admins through admin tools and logs	- Respond to requests for support - Conduct anonymized, aggregated analytics to improve Zoom's performance.	None

Category	Collection	Access	Use	Disclosure
Meeting metadata	Via Zoom meeting setup and participation: Data such as: • duration of meeting • participants' email address/name/other information entered • join/leave time of participants • meeting statistics/metrics • name of meeting • description of meeting • start date/time of meeting • chat status	• Zoom Support through admin tools and logs • SFU Zoom Admins through admin tools and logs • Account Owner through viewing Reports feature	• Provide dashboards and reports to customers. • Respond to requests for support.	None
User-generated content	Via Zoom meeting participation: Data shared while using the service: • chats • video • audio • polls • screen shares • annotations • whiteboard diagrams	• Zoom Support • SFU Zoom Admins • Zoom meeting participants, and account owner, through meetings, including in-meeting chats	• Save chat transcript locally (by host) • Store recordings locally (by host). SFU has turned on local recording for faculty and staff.	• Zoom meeting participants for collaboration purposes

2.6.2. Non-SFU Account Users and Free Account Users

Note: Non-SFU Account Users can include licenses purchased and held by SFU departments, i.e., are not part of SFU's enterprise licenses.

Category	Collection	Access	Use	Disclosure
Identifiers	Via user entry at Zoom account setup: • First name • Display name • Last name • SFU email address • Profile image • Physical address • Phone number • Approximate	• Zoom Support through admin tools • Account Owner Admin through admin tools • Account	• Create a user account • Communicate with a user • Respond to requests for support • Viewing a user's profile for identification	• Display name, phone number, location is viewable when attendees hover over your profile in desktop client. • Display name viewable by

Category	Collection	Access	Use	Disclosure
	location	Owner through self-service account management interface Attendees via participation in a session	and/or contact information	attendees in Zoom meetings via attendee list. Profile photo is viewable by all attendees in a session.
Employment information	Via user entry at Zoom account setup: - Department - Job title - Company	- Zoom Support through admin tools - Account Owner Admin through admin tools - Account Owner through self-service account management interface	- Create a customer account - Viewing a user's profile for identification and/or contact information	Department, job title, and location is displayed to other users when they hover over your profile icon in the Zoom desktop client.
User preferences	Via user entry at Zoom account setup; Service preferences and configuration such as enabling a waiting room, muting video/audio for attendees, etc.	- Zoom Support through admin tools - Account Owner Admin through admin tools - Account Owner through self-service account management interface	To provide user with choices for how to use/configure Zoom	None
Device and network information	Via Zoom meeting participation: Information on a user's device, network, and internet connection, such as: - IP address(es) - MAC address - Other device ID (UDID) - Device type - Operating system	Zoom Support through admin tools and logs	- Provide dashboards and reports - Respond to requests for support - Monitor performance of data centers and networks - Conduct anonymized,	None

Category	Collection	Access	Use	Disclosure
	type and version Client version		aggregated analytics to improve Zoom's service performance	
Usage information	Via Zoom meeting participation: Usage activities and other interaction with the service, such as whether a user switched between mobile client to desktop client, whether a user used VoIP or phone call, etc.	Zoom Support through admin tools and logs	- Respond to requests for support - Conduct anonymized, aggregated analytics to improve Zoom's performance.	None
Meeting metadata	Via Zoom meeting setup and participation: Data such as: - duration of meeting - participants' email address/name/other information entered - join/leave time of participants - meeting statistics/metrics - name of meeting - description of meeting - start date/time of meeting - chat status	- Zoom Support through admin tools and logs - Account Owner through viewing Reports feature	- Provide dashboards and reports to customers. - Respond to requests for support.	None
User-generated content	Via Zoom meeting participation: Data shared while using the service: - chats - video - audio - polls - screen shares - annotations - whiteboard diagrams	Zoom meeting participants through meetings, including in-meeting chats	- Store chat logs (for delivery and so you can review and search chat history) – may be local or cloud depending on configuration. - Store recordings, if explicitly requested by the host – may be local or cloud depending on configuration.	Zoom meeting participants for collaboration purposes
SFU credentials	Via user entry by account owner in	Zoom Support	Set up calendar and contact	None

Category	Collection	Access	Use	Disclosure
(for calendar and contacts sync feature)	account management interface: • SFU Email Address (with SFU Computing ID) • SFU Computing password	- through admin tools • SFU Zoom Admin through admin tools • Account Owner through self-service account management interface	sync between Zoom and SFU Mail	

2.6.3. Non-Account Users (i.e., Attendee Only)

Category	Collection	Access	Use	Disclosure
Identifiers	If joining by web: • Username If joining by phone: phone number, IP address, location, connection type.	• Zoom Support through admin tools • SFU Zoom Admin through admin tools • Account Owner through self-service account management interface • Attendees via participation in a session	• Viewing a user's profile for identification information	If joining by web: Username is viewable by the host as well as other attendees of the same meeting. If joining by phone: displays first three digits and last four digits; obscures middle 4 digits.
Employment information	None	None	None	None
User preferences	None	None	None	None
Device and network information	Information on a user's device, network, and internet connection, such as IP address(es), MAC address, other device ID (UDID), device type, operating system type and version, and client version.	• Zoom Support through admin tools • SFU Zoom Admin through admin tools	• Provide dashboards and reports • Respond to requests for support • Monitor performance of data centers and networks • Conduct anonymized,	None

			aggregated analytics to improve Zoom's service performance	
Usage information	Usage activities and other interaction with the service.	Zoom Support through admin tools and logs	- Respond to requests for support - Conduct anonymized, aggregated analytics to improve Zoom's performance.	None
Meeting metadata	Data such as: - duration of meeting - participants' email address/name/other information entered - join/leave time of participants - name of meeting - date/time of meeting - chat status	- Zoom Support through admin tools and logs - Meeting host through reports	- Provide dashboards and reports to customers. - Respond to requests for support.	None
User-generated content	Data shared while using the service: - chats - video - audio - polls - screen shares - annotations - whiteboard diagrams	Zoom meeting participants through meetings, including in-meeting chats	- Store chat logs (for delivery and so you can review and search chat history) – may be local or cloud depending on configuration. - Store recordings, if explicitly requested by the host – may be local or cloud depending on configuration.	Zoom meeting participants for collaboration purposes

2.7. Storage or Access outside Canada

Provide a brief description of whether the personal information can be accessed from outside Canada. For example, by a service provider that is repairing a system, or if the information is being stored outside Canada, for example, in the "cloud". If the data is stored within Canada and accessible only within Canada, please indicate this and describe with whom and where it is stored.

SFU's configuration of Zoom stores information on servers outside of Canada. Zoom's Privacy Policy requires users to consent to the disclosure of their personal information outside of Canada.

Zoom has stated that it is able to provide a configuration which stores data on servers exclusively located in Canada in the near future (estimated time of availability is December 2020). SFU is actively exploring these options to determine what cost these options will have on the usability and reliability of the service. Zoom employees will have the technical capability of accessing SFU data stored on Canadian servers for the purposes of troubleshooting and support.

The hosting location of communications services is handled differently from that of cloud recording services – i.e., hosting communication services in Canada is an option, whereas cloud recordings are stored on non-Canadian servers. On April 13, 2020, Zoom had announced that, starting April 18, 2020, paid Zoom administrators and account owners will have the option of opting in or out of specific data center regions, applicable only to data in transit. Zoom's announcement can be found at <https://blog.zoom.us/wordpress/2020/04/13/coming-april-18-control-your-zoom-data-routing/>. SFU's configuration for data in transit limits traffic to Canadian and US-based servers only.

Consent for Storage/Access Outside of Canada and Opt-Out Procedure

After a user authenticates via SFU's Central Authentication Service (CAS) with their SFU Computing ID and password, they will be presented with a prompt containing the collection notice and consent form. The user must select the "Accept" checkbox, then click a button to confirm, and the consent is stored on a file on a local server and retained indefinitely. If a user does not choose to accept, there is a "Reject" option, which prevents a user from proceeding with logging into Zoom.

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 in section 6.1 of this document ("Information Provided by Zoom to Third Parties"), it does not disclose the user name to these third parties.

If a user does not authenticate via SFU's Central Authentication Services (CAS), but is instead simply sent an invitation to join a meeting via a Zoom URL, the invitation will include a link to a collection notice and consent form.

The above consent process does not give the students a choice about whether to use Zoom, because there are no reasonable alternatives to access the meeting. However, the consent process ensures that students understand their options to anonymize themselves and reminds them about other precautions they can take to protect their privacy. Users can anonymize themselves to other participants by using a pseudonym, changing their display name, and not using the audio and video conferencing features within Zoom. More information on Zoom Privacy and Security in general and How to Anonymize My Identity in particular is available to users at <https://www.sfu.ca/itservices/technical/videoconferencing/zoom/privacy.html>. This link will be advertised to users.

Use for Exam Invigilation Purposes: Zoom may be used for exam invigilation purposes while other solutions are being explored for this purpose. Recommended practices are being developed. Further details are available at <https://www.sfu.ca/content/dam/sfu/itservices/videoconferencing/SFU%20Zoom%20Exam%20Proctoring.pdf>. This link will be advertised to users.

Administrative-related use cases: The above consent process applies to all administrative use cases. If the administrative meeting involves a participant who is a non-

employee, the consent model described above should be used. For example, if Zoom is used for student advising purposes, the student should be advised in writing of their option to identify themselves using only their first name, or a nickname.

Recording is a greater concern for administrative use cases. Unlike learning sessions, administrative meetings may collect or disclose very sensitive personal information. Accordingly, the PIA team recommends against recording of administrative meetings; the recording function should not be used if the meeting is intended to discuss or disclose any personal information. Where recording is used, IT Services has enabled settings in Zoom where Zoom notifies participants when a recording is initiated and requires each participant's consent. IT Services and the University Archives have developed recording guidelines which are available online at <https://www.sfu.ca/itservices/technical/videoconferencing/zoom/privacy.html>. This link will be advertised to users.

2.8. Data-linking Initiative

In FIPPA, "data linking" and a "data-linking initiative" are strictly defined. Answer the following questions to determine whether your initiative qualifies as a "data-linking initiative" under the Act. If you answer "yes" to all 3 questions, your initiative may be a data linking initiative. If so, you must comply with requirements under the Act for a data-linking initiative.	
1. Personal information from one database is linked or combined with personal information from another database	☒ Yes ☐ No
2. The purpose for the linkage is different from those for which the personal information in each database was originally obtained or compiled	☐ Yes ☒ No
3. The data linking is occurring between either: 1) two or more public bodies or 2) one or more public bodies and one or more agencies	☐ Yes ☒ No
If you answered "yes" to all three questions, please contact the Information and Privacy Coordinator or Officer to discuss the requirements of a data-linking initiative.	

2.9. Common or Integrated Program or Activity

In FIPPA, "common or integrated program or activity" is strictly defined. Answer the following questions to determine whether your initiative qualifies as "a common or integrated program or activity" under the Act. If you answer "yes" to all 3 questions, you must comply with requirements under the Act for common or integrated programs and activities.	
1. This initiative involves a program or activity that provides a service (or services)	☒ Yes ☐ No
2. Those services are provided through: 1) a public body and at least one other public body or agency working collaboratively to provide that service; or 2) one public body working on behalf of one or more other public bodies or agencies	☐ Yes ☒ No
3. The common or integrated program or activity is confirmed by a written agreement that meets the requirements set out in section 12 of the FIPPA Regulation (link to the Regulation and read section 12)	☐ Yes ☒ No
If you answered "yes" to all three questions, please contact the Information and Privacy Coordinator or Officer to discuss the requirements of a common or integrated program or activity.	

3. Collection, Use and Disclosure of Personal Information

3.1. Personal Information Flow Diagram / Table

Complete the table(s) below (if applicable). Include a personal data flow diagram (if one exists) as well as completing the table(s). See Schedule B for a list of the privacy rules. Use the hyperlink to the Act in Schedule B to identify the specific rule and cite the appropriate section number in the “Legal Authority” column.

3.1.1. User Data Flow

Personal Information Flow Table			
	Description/Purpose of Activity	Privacy Rule	Legal Authority
1.	User creates a new Zoom account by signing into SFU CAS at sfu.zoom.us. Identifiers and other data for account creation are collected by Zoom. User becomes an account owner.	Collection	26(c)
2.	Account owner sends an invitation to other individual(s) to participate in a Zoom session. Email addresses of recipients are collected in logs by Zoom.	Collection	26(c)
3.	Attendee accepts invitation with authenticated Zoom account.	Collection	26(c)
4.	Metadata about session is stored on Zoom server.	Collection, Storage outside Canada	26(c), 33.1(1)(b), M085
5.	If unrecorded, discussion flows through Zoom server without being stored there.	Access outside Canada	33.1(1)(p.1)
6.	If recorded, discussion is stored in the user's local storage.	Collection storage inside or outside Canada	26(c), 33.1(1)(b)
7.	Zoom administrators may monitor session, at SFU's request, in order to install, implement, maintain, repair, troubleshoot or upgrade the system. No data stored.	Access outside Canada	33.1(1)(p)
8.	Zoom retains account information only for as long as necessary to comply with legal obligations (e.g., tax compliance) but no longer than 10 years after account termination. User content is retained for the life of the account; however, users are free to delete this content at any time. When an account is terminated, user content is deleted after 60 days or as agreed with a client in a separate contract. Account information is information provided to Zoom when a user or company signs up for the	Retention	31

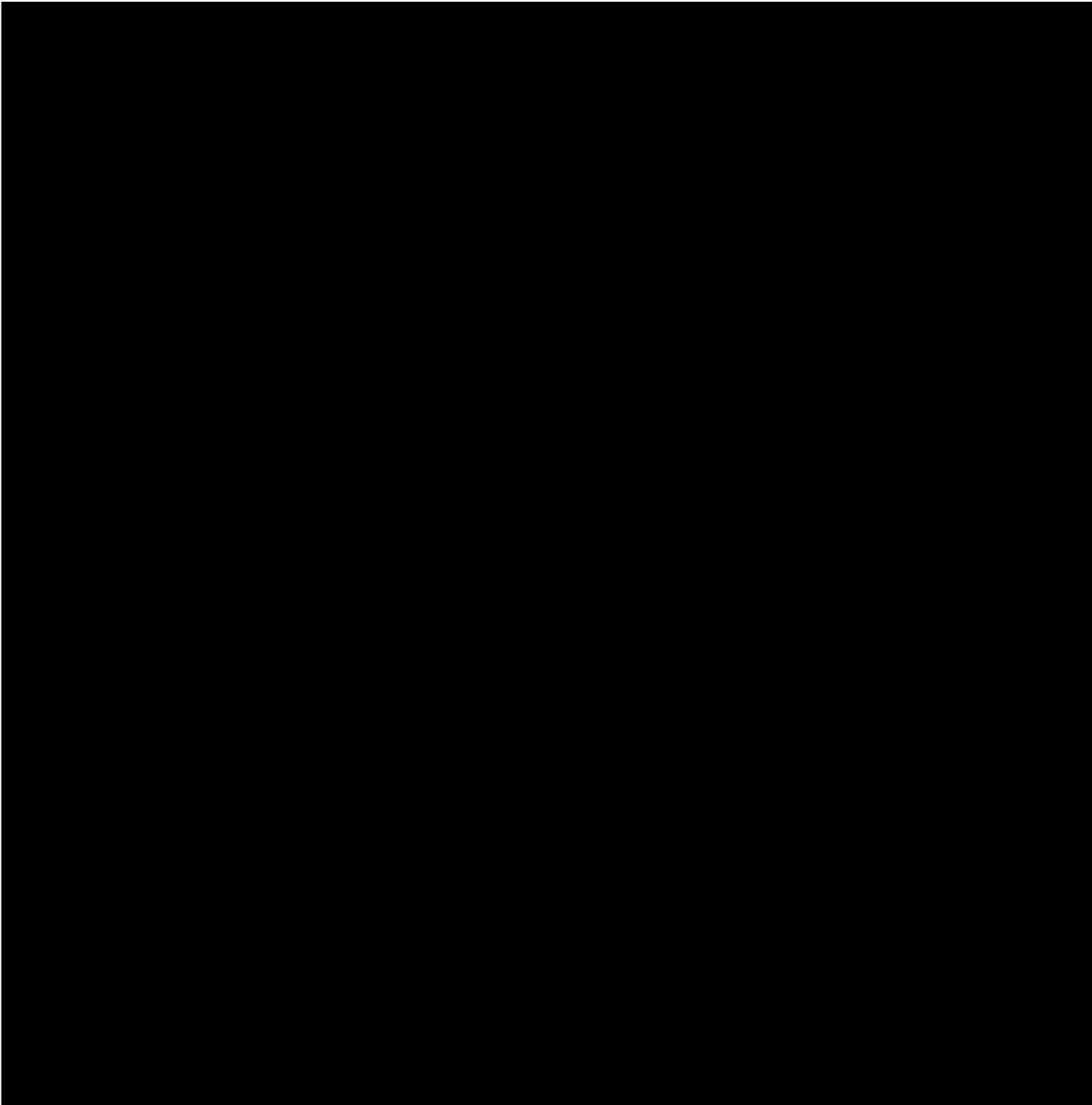
	Service. User content is information provided by the customer to Zoom through the usage of the service.		
--	---	--	--

3.2. Risk Mitigation Table

Complete the table(s) below. Describe the risk and the mitigation strategy. Use the terms “High”, “Medium” or “Low” to rate the “Likelihood” and “Impact” of each risk. In cases where the risks are substantially different for the individuals whose personal information is in SFU’s custody or under its control, complete a table for each group. In cases where the risks are substantially similar or the same, complete only one table.

3.2.1. Risks to User Data

Risk Mitigation Table			
Risk	Mitigation Strategy	Likelihood	Impact



3.3. Collection Notice

In order to allow individuals the ability to exercise their information rights with knowledge of how their information will be used, they must be notified at or prior to the time of collection. Section 27(2) of the Act requires that the individual from whom personal information is collected be told: a) the purpose for collecting it, b) the legal authority for collecting it, and c) the title, business address and business telephone number of an officer or employee of the public body who can answer the individual's questions about the collection.

Describe below how and when notice will be given to individuals. Include the specific collection notice(s) that will be used. Link to SFU's [collection notice templates](#).

3.3.1. Student, Instructor, and Employee Collection Notice and Consent Form

After a user authenticates via SFU’s Central Authentication Service (CAS) with their SFU Computing ID and password, they will be presented with a prompt containing the collection notice and consent form. The user must select the “Accept” checkbox, then click a button to submit/confirm their response, and the consent is stored on a file on a local server. If a user does not choose to accept, there is a “Refuse” option, which prevents the user from proceeding with logging into Zoom.

The notice presented to **SFU Zoom account users** is as follows:

British Columbia Freedom of Information and Protection of Privacy Act

Pursuant to Section 33.1(1)(b) of the British Columbia Freedom of Information and Protection of Privacy Act (RSBC 1996, c. 165), I give my consent for SFU Information Technology (IT) Services to disclose my personal information under the terms and conditions noted below.

1. The personal information to be disclosed is my first name, last name, information about my device, network, and internet connection (e.g., IP address(es), MAC address, device type, operating system, and client version), information about my usage of or the interaction with Zoom products, and other information I upload, provide, or create while attending a Zoom session.
 - This information will be held in a database at Zoom Video Communications, Inc. until I choose to stop accessing these services hosted by the vendor.
 - I may request that Zoom Video Communications delete my account at any time.
2. Personal information will be disclosed to Zoom, a web conferencing service provider located in the US with data centres deployed globally.
3. My personal information is disclosed in order to provision a personal account used to log into online video services hosted at Zoom Video Communication.
 - This account enables me to schedule video conferencing sessions for other SFU students, faculty or staff.
4. This consent to disclose my personal information remains in effect so long as I continue to schedule the above-mentioned video conferencing mechanisms.
 - I may revoke consent at any time by destroying my Zoom account hosted at <https://zoom.us/signin>

Zoom’s privacy policy is available [here](#).

Accessing Zoom Video Communications

Students

Please be advised that the personal information you disclose to Zoom (any information you provide to create an account, create a profile, attend a Zoom meeting, and any technical data that Zoom collects) is stored on servers located outside of Canada. Storage of your personal information outside Canada means the information resides in a foreign jurisdiction and will be subject to that jurisdiction’s laws. The data is stored indefinitely and privacy protection afforded by Canada’s privacy laws will not apply. You may wish to review the Zoom privacy policy before using the service.

SFU Employees

Please be advised that the personal information you disclose to Zoom (any information you provide to create an account, create a profile, attend a Zoom meeting, and any technical data that Zoom collects) is stored on servers located outside of Canada. The purpose of this storage is to provide you with and operate your Zoom account. Storage of your personal information outside Canada means the information resides in a foreign jurisdiction and will be subject to that jurisdiction’s laws. The data is stored indefinitely and privacy protection afforded by Canada’s privacy laws will not apply. You may wish to review the Zoom privacy policy before using the service. By choosing to use this service you consent to the storage of your personal information in this manner and for the purposes described above.

[Refuse] [I Accept the Terms of Use]

A form for collecting consent from **non-account users** (i.e., attendees choosing to use the web client to attend meetings/webinars without a Zoom account) is available on the IT Services website. The notice presented to non-account users is as follows:

British Columbia Freedom of Information and Protection of Privacy Act

Pursuant to Section 33.1(1)(b) of the British Columbia Freedom of Information and Protection of Privacy Act (RSBC 1996, c. 165), I give my consent for SFU Information Technology (IT) Services to disclose my personal information under the terms and conditions noted below.

1. The personal information to be disclosed is my display name, which may include my first and last name if I choose to enter them, information about my device, network, and internet connection (e.g., IP address(es), MAC address, device type, operating system, and client version), information about my usage of or the interaction with Zoom products, and other information I upload, provide, or create while attending a Zoom session. This information will be held in a database at Zoom Video Communications, Inc. until I choose to stop accessing these services hosted by the vendor. I may request that Zoom Video Communications delete your information at any time.
2. Personal information will be disclosed to Zoom, a web conferencing service

provider located in the US with data centres deployed globally.

- 3. My personal information is disclosed in order to participate as an attendee in online video services hosted at Zoom Video Communication.
- 4. This consent to disclose my personal information remains in effect so long as I continue to participate in the above-mentioned video conferencing mechanisms.

Zoom’s privacy policy is available [here](#).

Accessing Zoom Video Communications

Students

Please be advised that the personal information you disclose to Zoom (any information you provide to attend a Zoom meeting, and any technical data that Zoom collects) is stored on servers located outside of Canada. Storage of your personal information outside Canada means the information resides in a foreign jurisdiction and will be subject to that jurisdiction’s laws. The data is stored indefinitely and privacy protection afforded by Canada’s privacy laws will not apply. You may wish to review the Zoom privacy policy before using the service.

SFU Employees

Please be advised that the personal information you disclose to Zoom (any information you provide to attend a Zoom meeting, and any technical data that Zoom collects) is stored on servers located outside of Canada. The purpose of this storage is to provide you with access to Zoom sessions. Storage of your personal information outside Canada means the information resides in a foreign jurisdiction and will be subject to that jurisdiction’s laws. The data is stored indefinitely and privacy protection afforded by Canada’s privacy laws will not apply. You may wish to review the Zoom privacy policy before using the service. By choosing to use this service you consent to the storage of your personal information in this manner and for the purposes described above.

[I consent to the above terms of use]

4. Security of Personal Information

Describe below the specific measures that will be used to protect the personal information from unauthorized collection, access, use, disclosure, retention and disposal. See Schedule C for a list of common types of security measures.

4.1. Physical Security Measures

The Zoom application is hosted on external cloud-based commercial infrastructure sites. Zoom is hosted within AWS (Amazon Web Services) in the US.

4.2. Technical Security Measures

Under Zoom’s Privacy Policy webpage, the following is stated:

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:

- 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 the Advanced Encryption Standard (AES)
- Leverages the physical and environmental protection of Zoom’s 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

In early April, Zoom had corrected wording on its website and security whitepaper to remove its mention of “end to end encryption”.

4.3. Security Policies, Procedures and Standards

The usage of Zoom must be done in adherence to the following policies:

- GP 24 (“Fair Use of Information and Communications Technology”) <https://www.sfu.ca/policies/gazette/general/gp24.html>.
- I 10.4 (“Access to Information and Protection of Privacy”) <http://www.sfu.ca/policies/gazette/information/I10-04.html>
- I 10.5 (“Collection of Personal Information”) <http://www.sfu.ca/policies/gazette/information/I10-05.html>
- SFU’s Data Governance Policy (currently pending approval by the Board of Governors) may also be applicable. In summary, data governance ensures:
 - The right people are making decisions about data,
 - All users process accurate information,

- Data values are consistent across the institution, and
- Decisions are made based on accurate data.

Policies regarding student, faculty, and employee conduct should also be followed during participation in Zoom meetings and webinars.

4.4. Tracking Access / Access Controls

Describe the controls used to track access by authorized users of the personal information.

Access will be controlled through CAS logins with SFU Computing credentials. Any access to a Zoom account through CAS login will be tracked in system logs. A user’s eligibility to obtain an SFU enterprise license account will be determined by maillist membership and role (as indicated in Amaint), and will be updated with each sign-in through CAS SSO.

4.5. Information Classification Standard

(Note: this standard is under development – please leave this section blank). Using Information Technology Services’ standard for classifying the sensitivity, access restrictions and minimum-security requirements for information, identify the specific classification level that applies to this initiative.

Standard in the process of being developed.

5. Accuracy, Correction and Retention of Personal Information

5.1. Updating and Correcting Personal Information

Describe here (if applicable) the procedure to allow individuals to routinely update or correct their personal information using regular channels (e.g., a student uses the SIS to update a home address or telephone number, an employee uses the HAP system to update emergency contact information, etc.).

In the absence of a routine process, this requirement would default to SFU’s formal procedure [Requesting a Correction to Personal Information in University Records](#).

Zoom obtains data from Shibboleth (first name, last name, display name, department, and SFU email address) in a one-time import at time of account creation; no updates are pushed back to Shibboleth. As a result, if an individual chooses to update or correct their personal information in Zoom, they would do so by logging into their Zoom account and amending their profile details accordingly. This process is applicable to faculty, staff, students, and sponsored accounts.

5.2. Decisions That Directly Affect an Individual

Describe here (if applicable) how the information will be used to make decisions that directly affect an individual.

Scenarios where information will be used to make decisions that directly affect an individual include:

- exam invigilation to monitor student conduct,
- validation of student attendance for class participation evaluation,
- job interviews, and
- thesis defenses.

5.3. Records Retention and Disposal

Cite the approved SFU Records Retention and Disposal Authority (RRSDA) that apply to the records series generated through this initiative. Link to SFU’s [Directory of University Records](#) to determine if an approved RRSDA exists for these records.

If no approved RRSDA exists, describe how the records will be kept in the meantime. Note that if an individual’s personal information is used by or on behalf of SFU to make a decision that directly affects the individual, SFU must retain the personal information for at least one year after being used. This is to ensure that the affected individual has a reasonable opportunity to obtain access to that personal information.

Zoom has a process for records retention to ensure that Personal Information is retained for no longer than necessary to fulfill obligations or meet legal retention requirements. Zoom states in their privacy policy that they follow customers’ directions regarding personal data, and may store it, delete it, or disclose it at their direction. The privacy policy also states that Zoom will erase some or all of a user’s personal data from their systems on request unless it prevents Zoom from complying with regulatory obligations or impacts other legal matters, or requires extraordinary cost or effort. Zoom will accommodate requests to restrict further processing of personal data, which, in some scenarios, may require the deletion of the user’s account.

To make a request, a user may contact Zoom’s Privacy Team at privacy@zoom.us or by writing to the following address:

Zoom Video Communications, Inc.
Attention: Data Privacy Officer
55 Almaden Blvd, Suite 600
San Jose, CA 95113
US: 1-888-799-9666

Zoom will use your account information to verify your identity. If a user does not have an account, Zoom will ask the user to provide additional verification information.

Zoom retains account information only for as long as necessary to comply with legal obligations (e.g., tax compliance) but no longer than 10 years after account termination. User content is retained for the life of the account; however, users are free to delete this content at any time. When an account is terminated, user content is deleted after 60 days or as agreed with you in a separate contract. Account information is information provided to Zoom when a user or company signs up for the Service. User content is information provided by the customer to Zoom through the usage of the service.

SFU Admins can set custom retention periods and delete data as a self-service via in-product features and tools. Dashboard information is automatically deleted on a rolling 12-month period. Users are able to delete personal data of meeting and webinar participants as a self-service via in-product tools and technology.

Unless a meeting is recorded by the host, the video, audio, and in-meeting chat are not stored. Moreover, participants are notified through both audio and video when the host is recording a meeting through Zoom and have the choice to opt-in or leave the meeting. When the meeting is recorded, it is, at the host's choice (or as configured by the customer's admin settings), stored either locally on the host's machine or in the Zoom cloud.

Zoom deletes logs after 1 year from collection. Reports can be retrieved for the last 12 months, with a search range of up to one month at a time. If a meeting is not started in 30 days and is batch deleted by Zoom, the reports for the meeting are also deleted.

6. Further Information

6.1. Systematic Disclosures of Personal Information

Describe here (if applicable) any usual disclosures inside the University between the office with primary responsibility for the personal information and other SFU departments and programs. Also describe any usual disclosures outside the University between SFU and another public or private body (e.g., provincial, territorial or federal government ministry, department or agency; university or college; transit authority; law enforcement agency).

If SFU and one or more other parties have signed an Information Sharing Agreement, include a copy with this completed PIA. An Information Sharing Agreement sets terms and conditions on the collection, use, disclosure and protection of personal information by the parties to the agreement.

Usual Disclosures inside the University

Usual disclosures include names and email addresses for setting up or inviting attendees to a Zoom session. Personal information may be disclosed during a Zoom session by meeting attendees (e.g., personal views or opinions, work history, academic history, etc.).

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 their services, troubleshoot, and to improve its marketing efforts. While the disclosed data is not linked to a user name, it is potentially re-identifiable through Zoom's gallery view that displays thumbnails of participants in a grid format.

Recently, Zoom issued an update to its iOS app which stops it from sending certain pieces of 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. As far as the PIA team can determine, no such functionality exists in other operating systems.

In early April, Zoom had permanently removed the LinkedIn Sales Navigator App, which was found to have been disclosing names and email addresses to third parties without notifying or obtaining permission from the Zoom user.

6.2. Access for Research or Statistical Purposes

Describe here (if applicable) any usual disclosures of the personal information made by your department for a research purpose, including statistical research, and how you comply with [section 35 of the Act](#).

N/A

6.3. Personal Information Directory (PID) and Personal Information Banks (PIB)

The Personal Information Directory (PID) contains descriptions of the Personal Information Banks (PIBs) created and maintained by Simon Fraser University. A PIB is a collection of personal information that is organized or retrievable by the name of an individual or by an identifying number, symbol or other particular assigned to an individual. PIB entries are added to the Directory as PIB records series are identified and scheduled.

Cite the PIB that apply to the records series generated through this initiative. Link to SFU's [Directory of University Records](#) and search the Personal Information Directory to determine if a PIB description exists for these records.

If no PIB description exists, create one below using the outline described in the [Personal Information Directory](#).

The Zoom platform does not constitute a Personal Information Bank.

7. Coordinator of Information and Privacy Comments

7.1. Information or Materials Reviewed

The Coordinator will describe here any additional resources and authorities consulted when reviewing and commenting on the completed PIA.

I reviewed and considered:

1. Zoom's Privacy Policy
2. Zoom Video Communications Master Subscription Agreement
3. Zoom Video Communications End User License Agreement
4. Zoom Global Data Processing Addendum
5. UBC Privacy Impact Assessment (PIA 2020.03-51 Zoom)
6. Discussions and meetings with Melissa Luck, Project Manager and Mark Jutras, Service Owner, Videoconferencing

7.2. Conditions of Approval

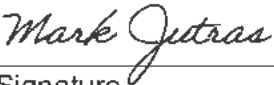
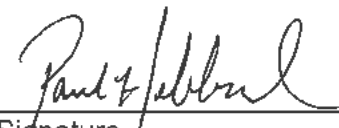
The Coordinator will describe here any recommended conditions to be considered by the University officer with delegated decision-making authority under the Act, who approves the completed PIA.

Recommended conditions are:

- 1. Any contemplated changes to or use of this software that differs from the description provided in this PIA (e.g., in the collection, use, disclosure or storage of personal information) must be reviewed by the Archives for compliance with FIPPA. IT Services must consult with the Archives and Records Management Department prior to implementing any proposed changes, including LMS integration and relocating SFU's Zoom instance to a Canadian Data Centre.
- 2. Encourage SFU departments and community members to use SFU's Zoom enterprise license instead of previously purchased or personal licenses. SFU's Zoom instance has been configured to maximize privacy protections.
- 3. Consent forms should be retained for a minimum of one year from the date of a user's last attended Zoom meeting.
- 4. SFU's Service Owner and Product Owner for Videoconferencing will monitor Zoom's terms of use for changes.
- 5. The possible risks of participation in SFU Zoom meetings by non-enterprise users will be updated and advertised on the SFU ITS website as developed.

8. Approval and Signatures

The undersigned confirm that they have taken reasonable steps to confirm that the contents of this PIA are accurate and complete.

Martin Pochurko		Oct 19, 2020
Insert position of delegated officer with FIPPA decision-making authority under SFU Policy I 10.02	Signature	Date
Mark Jutras		October 16, 2020
Insert position title of Service Owner (if applicable)	Signature	Date
Melissa Luck		October 16, 2020
Insert position title of Project Manager, Information Technology Services (if applicable)		
Paul Hebbard		October 14, 2020
Coordinator of Information and Privacy	Signature	Date

Schedule A

Definition of terms	
Access	Disclosure of personal information by the provision of access to personal information.
Anonymize	Present the results of a process in such a way that individuals whose personal information is contained in the records cannot be identified, and no linkages can be made between any personal information found in the records and personal information that is publicly available from other sources.
Authorized access	Occurs when a person has access to personal information in the custody or control of the University that is authorized by the Act.
Consistent purpose	A use of personal information is consistent with the purpose for which the information was obtained or compiled if the use: 1. has a reasonable and direct connection to that purpose, and 2. 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.
Contact information	Information that enables an individual at a place of business to be contacted; includes name, position title, business telephone number, business address, business email or business fax number of the individual.
Data linking	The linking or combining of personal information in one source with personal information in one or more other sources if the purpose of the linking or combining is different from: 1. the purpose for which the information in each database was originally obtained or compiled, and 2. every purpose that is consistent with each purpose referred to in paragraph (a).
Disclose	Reveal, show, expose, provide copies of, sell, give or tell. SFU may disclose personal information in its custody or under its control only as permitted under section 33.1, 33.2 or 33.3 of the Act.
Employee	A person employed for wages or salary by the University. In relation to SFU, includes: (a) a volunteer and (b) a service provider (see also the definitions for each of the latter terms).
Individual identifier	Information that would enable a third party to deduce the identity of the person concerned; examples include a person's name, Social Insurance Number, student number, employee number, address, date of birth (usually used in combination with other identifiers).

Instructor	Individuals responsible for the teaching of credit and non-credit courses including professors, associate professors, assistant professors, professors emeritus, adjunct professors, visiting faculty, practitioner faculty, post-retirement appointees, lecturers, instructors, teaching assistants, tutors and markers, faculty associates, in-service associates, associate members and program coordinators.
Personal information	Recorded information about an identifiable individual, other than business contact information, including but not limited to: 1. names, home addresses and telephone numbers; 2. age; 3. sex; 4. marital or family status; 5. identifying number; 6. race, national or ethnic origin; 7. colour; 8. religious or political beliefs or associations; 9. educational history; 10. medical history; 11. disabilities; 12. blood type; 13. employment history; 14. financial history; 15. criminal history; 16. images; 17. anyone else's opinions about an individual; 18. an individual's personal views or opinions; and, 19. name, address and phone number of parent, guardian, spouse or next of kin.
Record	Includes books, documents, maps, drawings, photographs, letters, vouchers, papers and any other thing on which information is recorded or stored by graphic, electronic, mechanical or other means, but does not include a computer program or any other mechanism that produces records.
Service provider	A person retained under contract to perform services for SFU or a person with whom an employee automatically enters into an agreement by virtue of using their product or service and in so doing accepts the service provider's terms of use.
Unauthorized collection, use, disclosure and disposal	Occurs when a person who has access, whether authorized or unauthorized, to personal information in the custody or control of the University, collects, uses, discloses and disposes of that information and it is not authorized by the Act.
Use	Employ information to accomplish a specific purpose.
Volunteer	A person who provides a service to the University without being paid.

Schedule B

[FIPPA table of contents](#)

Collection, Accuracy, Correction, Protection and Retention of Personal Information

Collection	Section 26	Purpose for which personal information may be collected
		1. Prescribes the only situations in which SFU is permitted to collect personal information 2. Collect only the minimum personal information related directly to and necessary for the particular purpose
	Section 27	How personal information is to be collected
		3. Prescribes that SFU must collect personal information directly from the individual the information is about except in very limited and specified circumstances 4. Prescribes when a collection notice is required and not required to be given to individuals
	Section 27.1	When personal information is not collected
		5. Describes the situation when personal information is received by SFU but not collected
Accuracy	Section 28	Accuracy of personal information
		1. Prescribes that SFU must make every reasonable effort to ensure that the personal information it uses is accurate and complete 2. Information collected by the University is often used to make a decision that directly affects the individual. Ensure this information is accurate because using out-dated information may result in serious consequences for the individual and the University
Correction	Section 29	Right to request correction of personal information
		1. Prescribes how SFU must handle a request made by an individual to correct her or his information 2. Where factual errors in personal information are identified, the University is responsible for making the appropriate corrections upon request. If the incorrect information was made available to a third party, the University is responsible for providing the corrected information to that third party

Protection	Section 30	Prescribes that SFU must protect personal information in its custody or under its control by making reasonable security arrangements against such risks as unauthorized access, collection, use, disclosure or disposal
		1. The media on which information is stored (paper or digital) must be considered when deciding what reasonable physical, technical and procedural security measures are necessary to adequately protect the personal information
	Section 30.1	Storage and access must be in Canada
		2. Prescribes that SFU must ensure that personal information in its custody or under its control is stored and accessed only in Canada except in very limited and specified circumstances
Retention	Section 31	Retention of personal information
		1. Prescribes that SFU must ensure that personal information is retained for at least one year after being used so that the affected individual has a reasonable opportunity to obtain access to that personal information

Use and Disclosure of Personal Information

Use	Section 32	Use of personal information
		1. Prescribes the only situations in which SFU may use the personal information it collects 2. Consider the difference between “use” (within the University office that collected) and “disclosure” (making information available to anyone else inside or outside the University)
Disclosure	Section 33	SFU may disclose personal information in its custody or under its control only as permitted under section 33.1, 33.2 or 33.3
		1. Describes the situations in which personal information may be released to another person. The circumstances under which personal information may be disclosed are prescribed in very specific and limited terms, therefore, it is important to confirm that one has legal authority to disclose personal information before doing so
	Section 33.1	Disclosure inside or outside Canada
		2. Prescribes the only situations in which SFU may disclose personal information inside or outside Canada

- Section 33.2 Disclosure inside Canada only
 - 3. Prescribes the situations in which SFU may disclose personal information inside Canada only

- Section 33.3 Disclosure of personal information in records available to public without request
 - 4. Prescribes the situation when SFU may disclose to the public a record that is within a category of records established under section 71(1)

- Section 35 Disclosure for research or statistical purpose
 - 5. Prescribes the situation when SFU may disclose personal information in its custody or under its control for a research purpose, including statistical research

Schedule C

Types of security measures	
Physical	1. SFU data centre and backup data centre are both located on SFU campuses in Canada 2. Locked doors 3. Key card and electronic access control devices 4. Securely stored computing equipment 5. Receptionist supervision 6. Physical barrier to the public 7. Staff only access 8. Alarm systems 9. After hours security patrol checks
Technical	1. Firewalls 2. Encrypted network transmission 3. Tiered network infrastructure 4. Identity assurance provided by SFU's main Systems of Record 5. Role-based user access assigned on a need-to-know basis 6. Log-on user ID and password (single sign-on) provided by SFU's Central Authentication Service (CAS) 7. Timed out computer sessions
Security Policy, Procedure and Standards	1. University Policies e.g., GP-24 Fair Use of Information Systems, I 10.04 Access to Information and Protection of Privacy, I 10.05 Collection of Personal Information, I 10.09 Retention and Disposal of Student Exams or Assignments, and I 10.10 Confidentiality Policy 2. Designation and authentication of authorized users is managed through SFU's Identity and Access Management (IDAM) infrastructure, which is registered with the Canadian Access Federation (CAF) 3. SFU's IDAM infrastructure is benchmarked against the InCommon assurance program (http://incommn.org), which certifies campuses, non-profits and research organizations to determine the accuracy of a user's electronic identity and help mitigate risk for the service provider. While InCommon certification is not available outside the US, the assurance program serves as a benchmark for international standards and best practices 4. SFU's Privacy Protection Schedule is included as part of a signed agreement with a service provider of digital storage when purchased through Procurement, which includes provisions relating to data ownership, use, disclosure, security, retention and confidential/permanent deletion 5. SFU has signed an Information Sharing Agreement with the public body describing the terms and conditions of their data-linking initiative or common or integrated program or activity 6. Authorized users of the IT system are made aware of protection of privacy rights and responsibilities by means of notices when logging onto the system;

	education by through the SFU website, workshops and advisory service; and/or signing SFU's Privacy and Confidentiality Agreement
	7. Personal information is retained and disposed of according to an existing Records Retention Schedule and Disposal Authority approved by the University Archivist
Tracking Access / Access Controls	1. IDAM infrastructure assures identity 2. Role-based access management infrastructure authorizes access 3. Auditable log files

Appendix A

Administrative Settings for Zoom Features

Default settings can be changed by the meeting host if not locked. Settings with “n/a” under the “Locked” column indicate that they cannot be locked.

A.01 Scheduling

Setting	Description	Default Setting	Locked
Video On	Host video Start meetings with host video on	Off	No
	Participants video Start meetings with participant video on. Participants can change this during the meeting.	Off	No
Audio Type	Options: - Telephone and Computer Audio - Telephone - Computer Audio	Telephone and Computer Audio	No
Join Before Host	Allow participants to join the meeting before the host arrives	Off	Yes
Personal ID	Use Personal Meeting ID (PMI) when scheduling a meeting	Off	n/a
	Use Personal Meeting ID (PMI) when starting an instant meeting	Off	n/a
	Only authenticated users can join a meeting The participants need to authenticate prior to joining the meetings, hosts can choose one of the authentication methods when scheduling a meeting.	Off	No
Watermark	Add watermark Each attendee sees a portion of their own email address embedded as a watermark in any shared content and on the video of the participant who is sharing their screen.	Off	No

Setting	Description	Default Setting	Locked
	Add audio watermark If an attendee records the meeting, their personal information will be embedded in the audio as an inaudible watermark.	Off	No
Zoom Logo	Always display "Zoom Meeting" as the meeting topic Hide actual meeting topic and display "Zoom Meeting" for your scheduled meetings	Off	Yes
Password	Require a password when scheduling new meetings A password will be generated when scheduling a meeting and participants require the password to join the meeting.	On	Yes
	Require a password for instant meetings A random password will be generated when starting an instant meeting.	On	Yes
	Require a password for Personal Meeting ID (PMI)	On	Yes
	Require a password for Room Meeting ID A password will be generated for Room Meeting ID.	On	No
	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	No
	Require password for participants joining by phone A numeric password will be required for participants joining by phone if your meeting has a password.	On	Yes
	Bypass the password when joining meetings from meeting list When Zoom Rooms join a scheduled meeting on its meeting list, users do not need to manually enter the meeting password.	On	No
Entry	Mute participants upon entry Automatically mute all participants when they join the meeting. The host controls whether participants can unmute themselves	On	Yes
Calendar	Calendar and Contact Integration Integrate your calendar and contact service, such as Google account, Outlook	Off	Yes
	Office 365 users can consent to enterprise applications accessing company data on their behalf If turned off, the Office 365 administrator will need to consent to calendar integrations on behalf of the company. As an administrator, please choose the same settings configured in Office 365.	On	n/a
Reminder	Upcoming meeting reminder	Off	No

Setting	Description	Default Setting	Locked
	Receive desktop notification for upcoming meetings. Reminder time can be configured in the Zoom Desktop Client.		
	Enforce to use OAuth 2.0 only for authenticate Office365 calendar integration Enabling this setting will force users and Zoom Rooms to authenticate calendar service.	Off	n/a

A.02 In the Meeting (Basic)

Setting	Description	Default Setting	Locked
Encryption	Require Encryption for 3rd Party Endpoints (H323/SIP) Zoom requires encryption for all data between the Zoom cloud, Zoom client, and Zoom Room.	On	No
Chat	Chat Allow meeting participants to send a message visible to all participants	On	No
	↳ Prevent participants from saving chat	Off	n/a
	Private chat Allow meeting participants to send a private 1:1 message to another participant.	On	No
	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	No
Sound	Play sound when participants join or leave	Off	No
	↳ Heard by host only	On	n/a
	↳ Record and play their own voice by phone	On	n/a
File Transfer	File Transfer Hosts and participants can send files through the in-meeting chat	Off	No
Feedback	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	No
	Display end-of-meeting experience feedback survey Display a thumbs up/down survey at the end of each meeting.	Off	No
Co-Host	Co-host Allow the host to add co-hosts. Co-hosts have the same in-meeting controls as the host	On	No
Polling	Polling Add 'Polls' to the meeting controls. This allows the host to survey the attendees.	On	No

Setting	Description	Default Setting	Locked
Put on hold	Allow host to put attendee on hold Allow hosts to temporarily remove an attendee from the meeting.	Off	No
Toolbar	Always show meeting control toolbar Always show meeting controls during a meeting	Off	No
Screen Share	Show Zoom windows during screen share	Off	No
	Screen sharing Allow host and participants to share their screen or content during meetings	On	No
	Who can share? Options: • Host Only • All Participants	All participants	n/a
	Who can start sharing when someone else is sharing? Options: • Host Only • All Participants	Host Only	n/a
	Disable desktop/screen share for users Disable desktop or screen share in a meeting and only allow sharing of selected applications.	On	No
Toolbar	Annotation Allow participants to use annotation tools to add information to shared screens	On	Yes
	Whiteboard Allow participants to share whiteboard during a meeting	On	No
	↳ Auto save whiteboard content when sharing is stopped	Off	n/a
Remote control	Remote control During screen sharing, the person who is sharing can allow others to control the shared content	On	No
Feedback	Nonverbal feedback Participants in a meeting can provide nonverbal feedback and express opinions by clicking on icons in the Participants panel.	Off	No
Rejoin	Allow removed participants to rejoin Allows previously removed meeting participants and webinar panelists to rejoin	Off	No

A.03 In the Meeting (Advanced)

Setting	Description	Default Setting	Locked
Q & A	Q&A in webinar Allow attendees to ask questions for the host and panelists to answer	On	No
Breakout room	Breakout room Allow host to split meeting participants into separate, smaller rooms	On	No
	↳ Allow host to assign participants to breakout rooms when scheduling	On	No
Remote support	Remote support Allow meeting host to provide 1:1 remote support to another participant	Off	No
Closed captioning	Closed captioning Allow host to type closed captions or assign a participant/third party device to add closed captions	Off	No
	Save Captions Allow participants to save fully closed captions or transcripts	Off	n/a
Video	Far end camera control Allow another user to take control of your camera during a meeting	Off	Yes
	Group HD video Activate higher quality video for host and participants.	Off	No
	Virtual background Allow users to replace their background with any selected image.	On	No
Guest	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.	On	No
	Auto-answer group in chat Enable users to see and add contacts to 'auto-answer group' in the Contact list on chat.	Off	No
	Peer to Peer connection while only 2 people in a meeting Allow users to directly connect to one another in a 2-person meeting.	On	n/a
	Only show default email when sending email invites Allow users to invite participants by email only by using the default email program selected on their computer	Off	No
	Use HTML format email for Outlook plugin Use HTML formatting instead of plain text for meeting invitations scheduled with the Outlook plugin	Off	No
	DSCP marking Determine classification for network traffic. Enable	Off	No

Setting	Description	Default Setting	Locked
	DSCP marking for signaling and media packets. (Default is 56 for audio, 40 for video, and 40 for signaling.)		
Audio	Allow users to select stereo audio in their client settings Allow users to select stereo audio during a meeting	Off	No
	Allow users to select original sound in their client settings Allow users to select original sound during a meeting	Off	No
Tracking	Attention tracking (removed by vendor) Let the host see an indicator in the participant panel if meeting/webinar attendee does not have Zoom in focus during screen sharing. This feature was removed by Zoom as of April 2, 2020 https://support.zoom.us/hc/en-us/articles/115000538083-Attendee-attention-tracking	n/a	n/a
Waiting Room	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.	On	No
	Show a "Join from your browser" link Allow participants to bypass the Zoom application download process, and join a meeting directly from their browser.	Off	No
Livestreaming	Allow live streaming meetings	Off	No
	Allow Skype for Business (Lync) client to join a Zoom meeting Allow internal or external Skype for Business (Lync) client to connect to a Zoom meeting	Off	n/a

A.04 Email Notification

Setting	Description	Default Setting	Locked
	When a cloud recording is available Notify host when cloud recording is available	On	No
	When attendees join meeting before host Notify host when participants join the meeting before them	On	No
	When a meeting is cancelled Notify host and participants when the meeting is cancelled	On	No
	When host licenses are running low	80%	No
	When an alternative host is set or removed from a	On	No

Setting	Description	Default Setting	Locked
	meeting Notify the alternative host who is set or removed		
	When someone scheduled a meeting for a host Notify the host there is a meeting is scheduled, rescheduled, or cancelled	On	No
	When the cloud recording is going to be permanently deleted Notify the host 7 days before the cloud recording is permanently	Off	No
	When the meeting duration exceeds the limit Notify the specified users when the meeting duration exceeds the limit	Off	n/a

A.05 Admin Options and Additional Settings

Setting	Description	Default Setting	Locked
	Blur snapshot on iOS task switcher Enable this option to hide potentially sensitive information from the snapshot of the Zoom main window.	On	No
	Display meetings scheduled for others If disabled, users will only see their meetings even if they have schedule-for privilege for others	On	n/a
	Use content delivery network (CDN) Allow connections to different CDNs for a better web browsing experience.	On	n/a
	↳ Default	Wangsu (China)	n/a
	Allow users to contact Zoom’s Support via Chat Show Zoom Help badge on the bottom right of the page	On	n/a
	Show one person meetings on Dashboard and Reports Meetings with only one person will also be displayed on dashboard and reports.	Off	n/a
	Direct call a room system Enable direct call to a room system from client	Off	No

A.06 Recording

Setting	Description	Default Setting	Locked
Local	Local recording Allow hosts and participants to record	Off	Yes
	↳ Hosts can give participants the permission	Off	Yes
Cloud	Cloud recording	Off	Yes

Setting	Description	Default Setting	Locked
	Allow hosts to record and save the meeting / webinar in the cloud		
	Automatic recording Record meetings automatically as they start	Off	Yes
	Prevent hosts from accessing their cloud recordings By turning on this setting, the hosts cannot view their meeting cloud recordings. Only the admins who have recording management privilege can access them.	Off	Yes
	Cloud recording downloads Allow anyone with a link to the cloud recording to download	Off	Yes
	IP Address Access Control Allow cloud recording access only from specific IP address ranges	Off	No
	Only authenticated users can view The viewers need to authenticate prior to viewing the cloud recordings, hosts can choose one of the authentication methods when sharing a cloud recording.	Off	No
	Require password to access shared 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	On	No
	Auto delete cloud recordings after days Allow Zoom to automatically delete recordings after a specified number of days	On	No
	The host can delete cloud recordings Allow the host to delete the recordings. If this option is disabled, the recordings cannot be deleted by the host and only admin can delete them.	On	No
	Auto delete cloud recordings after days Allow Zoom to automatically delete recordings after a specified number of days	On	No
	Allow recovery of deleted cloud recordings from Trash Deleted cloud recordings will be kept in trash for 30 days. These files will not count as part of the total storage allowance	Off	n/a
Disclaimer	Recording disclaimer Show a customizable disclaimer to participants before a recording starts	On	No
	- Ask participants for consent when a recording starts - Ask host to confirm before starting a recording	On	No

Setting	Description	Default Setting	Locked
	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. If participants join the audio from telephone, even if this option is disabled, users will hear one notification message per meeting.	On	No

A.07 Telephone

Setting	Description	Default Setting	Locked
	Toll Call Include the selected numbers in the Zoom client and the email invitation via the international numbers link.	On	No
	3rd Party Audio Users can join the meeting using the existing 3rd party audio configuration	Off	No
	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	No
	Global Dial-in Countries/Regions Click the Edit icon to choose countries/regions that frequently have participants who need to dial into meetings.	Canada	No

A.08 Security and Sign-On Methods

Setting	Description	Default Setting	Locked
	Only account admin can change pro users' Personal Meeting ID and Personal Link Name	On	n/a
	Allow importing of photos from the photo library on the user's device	On	n/a
	Hide billing information from administrators Allows only the account owner to see billing information	On	n/a
	Users need to sign in again after a period of inactivity - Set period for inactivity on the web - Set period for inactivity on Zoom client	On; 10 minutes for both settings	n/a
	User need to input Host Key to claim host role with the length of numbers	6	n/a
	Sign in with Two-Factor Authentication By enabling this setting, users need to sign in again	Off	n/a

Setting	Description	Default Setting	Locked
	to start using two-factor authentication		