Securing Your Zoom Meetings

Due to recent occurrences of "Zoom bombing" where intruders into a meeting have caused disruption, or worse, used it as a platform for hate speech and hate crimes, we are urging you to take action. In the coming days UCSF IT will be making changes to Zoom's default settings to require passwords on all meetings, but that will not protect meetings that are already on the calendar. The instructions below will guide you through the steps to protect your existing scheduled Zoom meetings.

Set a meeting password

Follow the instructions below. You must *reschedule* any existing meetings you wish to protect once making these changes to your account.

1. Cancel the meeting you want to protect, and let the participants know a new inviting will be sent.
2. If you were previously using a Personal Meeting ID (PMI), discontinue, and use the generated Zoom meeting ID and password.
3. Log in to your Zoom account settings, toggle **Require a password when scheduling new meetings** on to the right

4. Reschedule and send the new meeting invite to your trusted participants (mostly likely in email or via a calendar invite). Learn about meeting IDs and how to generate a random meeting ID by using Zoom's "schedule" feature;
   a. If your need to publicize your event online, post only the meeting ID and then separately send the password to vetted participants before the meeting.

Here is more information about additional Recommended Security Settings for Zoom.

Setting a Personal Meeting ID (PMI) password

Avoid using your Personal Meeting ID **(PMI)** to host events. Your PMI is essentially one continuous meeting and people can pop in and out at any time. Protect your PMI for other meetings by adding a password.

Follow the instructions below. You must *reschedule* any existing meetings you wish to protect once making these changes to your account.
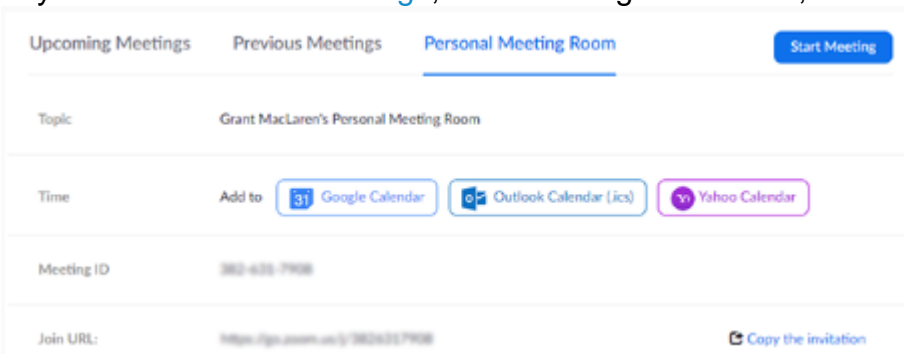
1. Cancel the meeting you want to protect and let the participants know a new inviting will be sent.

UCSF Data Classification – **P2 Internal Use Only**

UCSF Information Technology
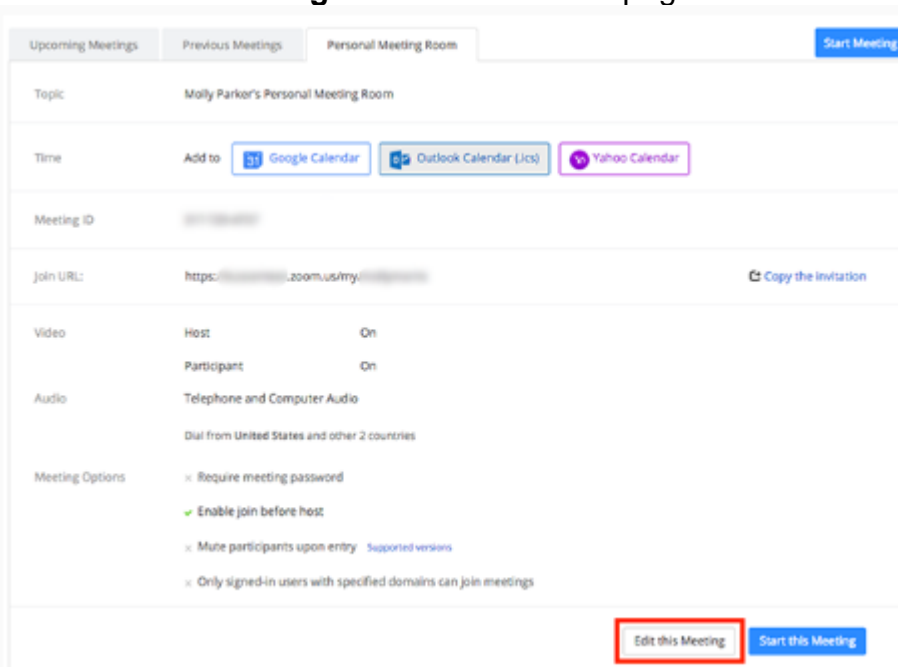
Securing Your Zoom Meetings

2. Log in to your [Zoom account settings](#), toggle **Require a password for Personal Meeting ID (PMI)** on to the right and select **All meetings using PMI**

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. The Personal Meeting ID (PMI) meetings are not included.

Require a password for instant meetings
A random password will be generated when starting an instant meeting

Require a password for Personal Meeting ID (PMI)
○ Only meetings with Join Before Host enabled
● All meetings using PMI

3. In your [Zoom account settings](#), click Meetings on the left, then click **Personal Meeting Room**

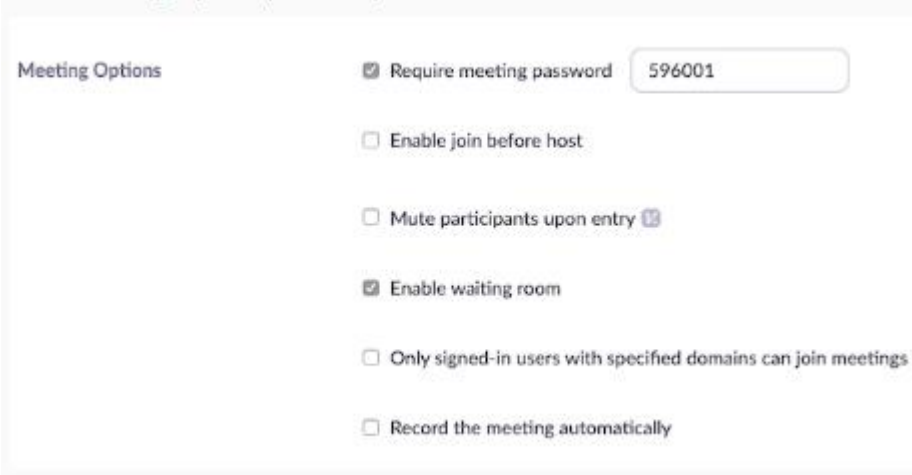|	
Upcoming Meetings	Previous Meetings	**Personal Meeting Room**	Start Meeting

Topic	Grant MacLaren's Personal Meeting Room
Time	Add to [31] Google Calendar Outlook Calendar (.ics) Yahoo Calendar
Meeting ID	382-631-7908
Join URL:	https://go.zoom.us/j/3826317908 Copy the invitation

4. Click **Edit this Meeting** at the bottom of the page

Upcoming Meetings	Previous Meetings	Personal Meeting Room	Start Meeting
Topic	Molly Parker's Personal Meeting Room		
Time	Add to [31] Google Calendar Outlook Calendar (.ics) Yahoo Calendar		
Meeting ID			
Join URL:	https://_____.zoom.us/my/_____ Copy the invitation		
Video	Host	On	
	Participant	On	
Audio	Telephone and Computer Audio		
	Dial from United States and other 2 countries		
Meeting Options	× Require meeting password		
	✓ Enable join before host		
	× Mute participants upon entry Supported versions		
	× Only signed-in users with specified domains can join meetings		

Edit this Meeting   Start this Meeting

UCSF Information Technology

Securing Your Zoom Meetings

5. Under **Meeting Options**, edit the password. Make it something that is <u>not easily guessable</u> (123456 and 444444 are bad) as this password is set until you change it.

6. Click **Save.**

UCSF IT is in direct contact with Zoom regarding concerns over their privacy and security shortcomings. We are deploying the latest software updates and reviewing our enterprise Zoom settings to make sure we provide the safest Zoom environment we can. UCSF IT will continue to monitor for news of new privacy or security flaws in Zoom and address them accordingly.

UCSF Data Classification – **P2 Internal Use Only**