ZOOM APP
SECURITY SETTINGS AND RECOMMENDATIONS

01 SET MEETINGS TO PRIVATE

02 SUGGESTIONS FOR CREATING OR SHARING A MEETING

03 AVOID SHARING CONFIDENTIAL INFORMATION

04 MAKE SURE THAT THE LATEST VERSION IS USED

05 LOG-OUT IF YOU ENCOUNTER ABNORMAL CONDITIONS

06 VIDEO RECORDING OF THE MEETINGS

07 IDENTIFY PARTICIPANTS
ZOOM APP
SECURITY SETTINGS AND RECOMMENDATIONS

08 SET A RANDOM ZOOM MEETING ID

09 SET A MEETING PASSWORD

10 DISABLE “ENABLE JOIN BEFORE HOST”

11 USE WAITING ROOM FUNCTION

12 REMOVE ZOOM MEETING PARTICIPANTS

13 LOCK MEETING

14 RESTRICT SCREEN SHARING
01 SET MEETINGS TO PRIVATE
Users can set the meeting to "Private" through two options, including asking participants to join the meeting with password, or enabling the "Waiting Room" function to control the entry of participants.

02 SUGGESTIONS FOR CREATING OR SHARING A MEETING
- Use a different meeting ID and password in each meeting.
- Share the meeting link privately with participants (for example by email) to ensure that the meeting link is private.
- Don’t share meeting links on social media platforms to avoid the links being searched publicly.

03 AVOID SHARING CONFIDENTIAL INFORMATION
During the meeting, avoid sharing or discussing confidential information or message.
SECURITY SETTINGS AND RECOMMENDATIONS

04 MAKE SURE THAT THE LATEST VERSION IS USED
- Keep ZOOM updated to the latest version.
- Update the operating system frequently.
- Install anti-virus software and keep its definition files updated.
- Only download the software from the official website or official app store.

05 LOG-OUT IF YOU ENCOUNTER ABNORMAL CONDITIONS
If you encounter any abnormal conditions during the meeting, you should immediately log out from all ZOOM accounts and change the account password.

06 VIDEO RECORDING OF THE MEETINGS
If the host wants to record the meeting, he/she should firstly notify all participants and keep the video clips properly.

07 IDENTIFY PARTICIPANTS
Participants should use identifiable names to make it easier for the host to identify participants.
SET A RANDOM ZOOM MEETING ID

When you are scheduling a meeting, click the "Generate Automatically" option and it will randomly generate a meeting ID to avoid exposure of your personal meeting ID.
SET A MEETING PASSWORD

When you are scheduling a meeting, select "Require Meeting Password", and then specify a strong password. Participants are required to use this password to join your meeting.
10 DISABLING "ENABLE JOIN BEFORE HOST"

This option allows participants to join the meeting before the host joins. However, if you select this option, the first participant entering the meeting will automatically become the host of the meeting, who has complete control of the meeting settings.

When scheduling a meeting, disable "Enable join before host" under Advanced Options.
USE WAITING ROOM FUNCTION

When scheduling a meeting, "Enable Waiting Room" function allows the host to control when a participant joins the meeting.

**Advanced Options** -
- **Enable waiting room**
- **Enable join before host**
- **Mute participants on entry**
- **Automatically record meeting on the local computer**
REMOVE ZOOM MEETING PARTICIPANTS
If necessary, you can remove a participant from the meeting. Select "Manage Participants" and choose the participant who needs to be removed from the participant list, then click "More" option and select "Remove".
“Lock Meeting” function can prevent anyone new from joining. Select "Manage Participants" and click "More" option under the list of participants, then select "Lock Meeting".
RESTRICT SCREEN SHARING

The meeting can be restricted so that only the host of the meeting can share their screen. Select the arrow next to "Share Screen" and select "Advanced Sharing Options", then click “Only Host” in the “Who can share?” option.

FOR MORE CYBER SECURITY TIPS, PLEASE VISIT CYBERSECURITYCAMPAIGN.COM.HK
Reference

1. Zoom Help Centre <Meetings & Webinars>
https://support.zoom.us/hc/en-us/categories/201146643-Meetings-Webinars

2. HKCERT <HKCERT proposes 10 measures to secure Zoom Meetings>
https://www.hkcerc.org/my_url/en/blog/20040201

3. Privacy Commissioner for Personal Data, Hong Kong <Zoom Data Security Incident>

4. Education Bureau <Using e-learning platforms in combination with flipped classroom strategy to support student learning at home>