For research conversations researchers must take steps to protect calls made using Pro accounts.

Before the Meeting:

- https://zoom.us/meeting/schedule to set up a meeting.
- Avoid sharing meeting links on social media or public outlets (unwanted participants may join or lurk in a meeting that they have no intentions of participating in).
- Avoid using Personal Meetings ID (PMI) to host public events - Your PMI is a permanent meeting room that anyone can pop into and out of at any time
- Introduce a Waiting Room - The Waiting Room is a virtual staging area that allows you to invite guests when you are ready for them. As of April 4. 202, this is a default setting.
- Introduce a password to gain access to the meeting room. This is especially important when the research topic is sensitive. As of April 4. 202, this is a default setting.

During the meeting:

- Ensure that endpoint encryption is enabled. You can learn how to do that here: https://support.zoom.us/hc/en-us/articles/201362723/
- Lock the meeting - By locking the meeting after it has started, no new participants can join.
- Remove participants – as a host or co-host you can remove any participant at any time.
- Manage Screen Sharing - To prevent random people from taking over sharing, restrict sharing to the host.
- Mute participants to protect privacy if appropriate:
- Disable private Chat prevents participants from receiving unwanted messages during a meeting
- Disable annotation if appropriate -

Video recording

1. Researchers must disable cloud recording. You can learn how to do that here: https://support.zoom.us/hc/en-us/articles/203741855-Cloud-Recording
2. Researchers must disable automatic recording. You can learn how to do that here: https://support.zoom.us/hc/en-us/articles/202921119-Automatic-Recording
3. Disable the video if you do not require the video feature for your project. The hosts can block the video capacity of the participant to prevent unwanted, distracting, or inappropriate gestures on video
4. If you are using local recording, ensure the recordings are stored on your host computer. You can learn how to do that here: https://support.zoom.us/hc/en-us/articles/201362473-Local-Recording.
    - hosts should log into their account and then click on '**my account'**, '**settings'**, and click on the '**recording'** tab. The following options should be set:
    - **Local recording** should be 'on'
    - **Hosts can give participants the permission to record locally** should be 'off'
    - **Cloud recording** should be 'off'
    - **Automatic recording** should be 'off'
    - **IP Address Access Control** should be 'off'
    - **Recording disclaimer** should be set to 'on'.
    - **Ask participants for consent when a recording starts** should be set to 'on'.
    - **Ask host to confirm before starting a recording** should be set to 'on'.

- When recording a meeting, which is initiated from within the meeting client, select '**Record on this Computer'** (recordings should not be stored on the Zoom cloud servers). Meeting hosts should be aware that even though you have selected a local recording, some caching of data may be done at the server to allow for the local recording. **All participants should be aware that they are being recorded, and should have given their consent for this**