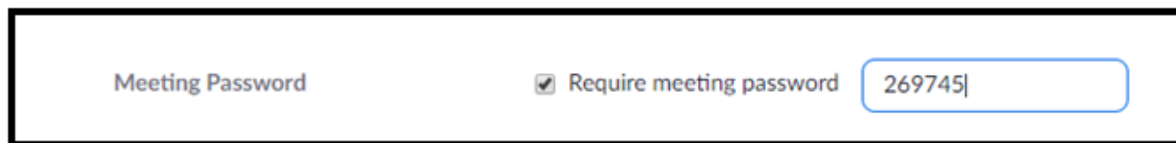# Security and Best Practices for Zoom

To prevent uninvited participants in your Zoom meetings and to enhance security, we recommend the following practices. Please be mindful of the information shared or discussed so that you do not violate any HIPAA or FERPA privacy rules. Always refer to UF Privacy statement to ensure that your Zoom practices are consistent with the UF policies and the laws and regulatory practices of the State of Florida, https://privacy.ufl.edu/privacy-policies-and-procedures/onlineinternet-privacy-statement/.

Setting a Meeting Password

If you would like to increase the security of your Zoom session, we recommend that you set a password for the session. When forwarding the password, remind them not to share it with others.

When scheduling a meeting in Zoom, enable the option "Require meeting password." A password (a six-digit number) will then be automatically generated for you, or you may change this to a password of choice. Before participants can join your session, they will be asked to enter this password.

Removing a Participant from a Zoom Session

As a host, you are able to manage your participants including removing someone from a Zoom session. Here is how.

1. If the **Participants** panel is not visible, click **Participants** on the Zoom toolbar.
2. Next to the person you want to remove, click **More**.
3. From the list that appears, click **Remove**.

Locking Your Session

Zoom allows the host or co-host to lock the meeting. You can do so if desire once all your attendees have joined. Once locked, no additional participants can join even if they have the meeting ID and password.

1. If the **Participants** panel is not visible, click **Participants** on the Zoom toolbar.
2. At the bottom of the **Participants** panel, click **More**.
3. From the list that appears, click **Lock Meeting**.

Unlock the meeting following these same steps.

When a meeting is locked, no one can join, and you (the host or co-host) will NOT be alerted if anyone tries to join, so do not lock the meeting until everyone has joined.
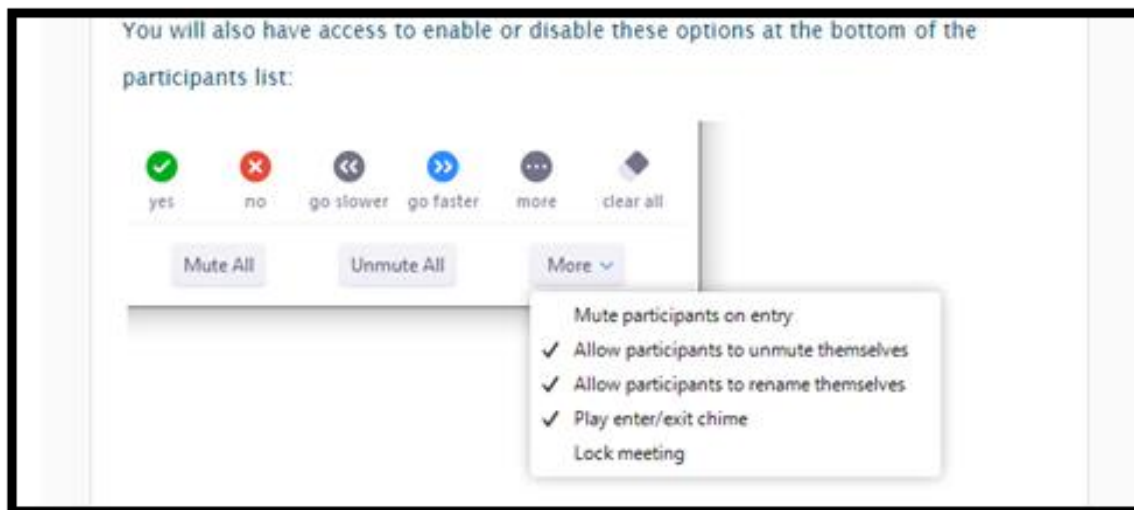
Best Practices for Zoom Teleconference for Staff

Below are best practices to make sure your Zoom video and audio conferences run smoothly.

- Mute your microphone unless you are actively talking. On the Zoom tool bar, you can click on the microphone icon to mute/unmute yourself.
- Disable your video by default to minimize the bandwidth
- Assume you are always on camera and audible (even if you think you are muted or video-disabled)
- Avoid any side-conversations with others outside the session to minimize distraction among remote participants
- Be careful not to talk over others. Politely wait your turn and if you are talking for a length of time, frequently pause to let others ask questions or seek clarification
- Minimize environmental or background noise by avoiding tapping pencils, moving papers around, setting coffee cups down on table-tops, tapping on keyboards, etc. These could be a major distraction and very unpleasant to others in the session.
- When conducting a video teleconference
  - make sure to dress professionally
  - situate yourself in a quiet room or location and isolate yourself from others in your household
  - prepare beforehand and have notes (or talking points) before the conference starts
  - take notes on "action items" during the conference whenever you are assigned tasks
  - be succinct and keep it short. Move any questions or issues that do not require live interaction to "offline."