From: OIT

Colleagues,

Zoom is a powerful web conferencing tool that enables remote work and frequent collaboration. With significantly increased usage during the spring quarter, it is necessary to get acquainted with available options and select the most suitable [configuration](#) for your meetings that maintains the privacy of the participants, as well as the security of the information shared.

Control who can join your meeting

- Don't share the [Meeting ID](#) or link publicly (i.e. calendar) where non-attendees may have access
- If hosting a public meeting, choose a different Meeting ID than you normally use for private meetings
- Consider using a [password](#) (shared privately) or the [waiting room](#) feature to control who can join your meeting
- Disable [Join Before Host](#) to prevent others from causing trouble before you start the meeting
- When possible, use the [Only authenticated users can join meetings](#) feature

Control what your meeting attendees can do

- Enable and give [co-host privileges](#) to a trusted moderator to help [manage participants](#) in the meeting
- Prevent participants from **screen sharing** by default
- Disable **chat** or file sharing unless needed
- **Mute** participants unless needed in public meetings
- Be familiar how to **remove** a participant and **lock** a meeting if needed
- It is extremely important to learn how to [manage participants in a meeting](#)

Set up privacy controls

- [Mute audio and disable video](#) by default when joining a meeting
- Enable a [Virtual Background](#) for meetings with video enabled
- Enable [Consent to be Recorded](#) to ensure all participants are properly [notified](#) before a host recording starts

- Disable participants from saving [cloud](#) or [local](#) recordings of the meeting
- Ensure [encryption](#) stays enabled

Please reach out to the OIT Help Desk at oit@uci.edu with any questions.

Sarkis Daglian, M.B.A.
Director, Client Services
Office of Information Technology