Zoom Security Information

Please read this article which goes over meeting settings in more detail, and this article which contains information on how best to secure your meetings.

We suggest that you take special caution around the following areas:

- Do not share meeting links in social media or public websites. Use your VSC provided email direct to send Zoom links and/or passwords to registered training participants. Please copy your Resource Advisor on the email in case questions arise and participants are not able to reach you.

- Consider instituting a waiting room or password. With a waiting room, those looking to join your meeting will be placed into holding until a host or co-host allows them access. A password prevents anyone from joining a meeting without both the meeting room link and the password.

- Consider using the schedule option in the Zoom to schedule your meetings. This will create a unique meeting ID for a series of meetings. For example, if you set a recurring meeting, all training sessions in a series will have the same meeting ID, but any meetings outside of this recurring meeting will not share the same meeting ID.

- Set your meetings to mute all participants upon entry. This will minimize distractions and prevent unwanted noise from interfering with your meeting.

- To protect participant privacy, do not record trainings.

- Make sure you are running the latest version of the Zoom client. Click the initials or your avatar image in the upper right of the client and choose “check for updates”. If you have concerns or questions around the use of zoom, please reach out to your local helpdesk at https://helpdesk.vsc.edu