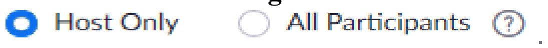
SOUTHWESTERN COLLEGE

Zoom Security Checklist

Please use discretion when utilizing security settings for all meetings.

As Southwestern College continues to work remotely users should take appropriate measures and actions to secure their video conference sessions. With “Zoom Bombing”, “High Jacking” and “Gate-Crash” on everyone’s mind, host should utilize and manage Zoom tools and features to help counter uninvited guest. The following is a checklist that will aid in preventing unwanted participants or inappropriate content from being broadcast. Please take the time to view and familiarize yourself with Zoom and its security settings. Simple adjustments and management can help avoid security risks.

Security Settings Guidelines:

- **Do not use your (Personal Meeting ID) to host *public events***. Your PMI is essentially one continuous meeting and people can pop in and out all the time.
- **Join Before Host**: Avoid (Join before Host) to prevent participants coming into the meeting before the Host.
- **Screen sharing:** Enable, only if the host wants to share their screen or content during meeting. Avoid allowing “all participants” to share (Security Risk). **Settings > In Meeting (basic) > scroll to “screen sharing”**
  Who can share? 
  ● Host Only ○ All Participants ? .
- **Set Passcode:** Meetings and webinars can require passcodes for an added layer of security. (How to set Passcode) at the individual meeting level or enabled at the user, group, or account level for all meetings and webinars.
- **Chat**: If disabled, the Host and Co-host will not be able to chat with each other or with participants. This feature prevents anyone from getting messages during the meeting. If enabled, ***avoid clicking on unverified links that may appear in Chat windows*.**
- **Consider using meeting registration:** Meeting registration requires attendees to register their name and email address prior to being emailed a link to join the session.
- **Only authenticated users can join meetings**: This feature will require users to sign into Zoom prior to joining the meeting.
- **Embed passcode in invite link for one-click join**: Should be avoided for ***public events***. The passcode will be encrypted and included in the invite link to allow participants to join with just one click without having to enter the passcode
- **Turn off annotations by participants*:*** Annotations allow participants to write on the screen. This feature can be disabled during the session while in screenshare mode or in profile settings

- **Participants Video:** If enabled**,** participants can turn video on during a meeting. The host or co-host can stop the video individually by hovering over the name "More"> "Stop Video" or by disabling "Start Video" in the security panel Security to stop video for all participants.
- **File Transfer:** Disable to prevent participants from sharing files with others.
- **Whiteboard:** Disable to prevent participants from sharing a whiteboard.
- **Allow removed participants to rejoin**: Disable this feature, this will prevent previously removed meeting participants and webinar panelists to rejoin. To remove a participant from the meeting, hover over the name, then select 'Remove' from the 'More' menu. Attendees can also be removed from the 'Waiting Room'.
- **Waiting Room**: Make sure (Waiting Room) is enabled, participants will be held in a room outside of the meeting while the Host/Co-Host prepare prior to greeting participants. This feature will require the host or co-host to admit participants individually or all at once.

  The "Waiting Room" announcement screen can also be customized for each unique conference to advise participants that they are in the correct meeting.
- **Report participants to Zoom**: Enable, Hosts can report meeting participants for inappropriate behavior to Zoom's Trust and Safety team for review. This setting can be found on the Security icon on the meeting controls toolbar or by hovering over the violator(s) name.
- Webinar: SWC has one (1) Webinar license that can accommodate 500 attendees, this method should be considered for public events with limited interaction or anticipated attendees beyond our licensed 300 capacity. Webinar can be used to present content in a manner that will allow attendees to listen-in and only engage via (chat, Q&A, polling raised raise hand).

Security tips during live meetings:

- Mute all participants upon entry.
- For more control or public events consider **disabling** allowing participants to unmute themselves located in the security panel. If participants wish to speak, they can type in the chat box or raise their hands. The host can then choose to unmute the requester at their discretion.
- Consider locking the meeting after a certain time. This will prevent individuals joining after meeting is locked.
  a. **Pro**: This prevents individuals from randomly joining late if they discover your session ID after the session begins.
  b. **Con**: participants cannot join the session late or rejoin if they have a technology problem.
- If you experience a disturbance during the meeting, the host can press "**Suspend Participant Activities"** located in the Security panel. This will immediately suspend all

participant activities, which will mute all video and audio, stop screen sharing, end all breakout rooms, and pause recording. This feature will also allow the host to report disruptive individuals/Zoom bombers to Zoom's security team. Must have 5.4.3 version and above.

- For inappropriate profile pictures the host can enable "Hide profile pictures" located in Security panel.
- The host can remove or report a participant by hovering over their name More>Remove or Report.
- If you suspect suspicious activity from a user, you can "Pin" (More>Pin) that participant to monitor their behavior. Pining someone will not be viewed by other participants or the notify the user pinned.
- ***Avoid clicking on unverified links that may appear in Chat windows***

Recording disclaimer**:** Attendees can be prompted to provide their consent to be recorded in a meeting or a webinar. If the recording disclaimer is enabled, attendees will receive a notification when a recording starts or if they join a session that is already being recorded. The attendee can either consent to stay in the session or leave.

Please remember that every meeting is unique and will require adjustments as needed, this checklist should be used as a reference and a guide to secure your video conference sessions. Make sure to always stay up to date on the latest application updates **(Zoom download center)** current version: Version 5.5.2 (12494.0204) 2/08/21**.** For additional information visit SWC Zoom page: https://www.swccd.edu/administration/institutional-technology/applications-and-software/zoom/index.aspx

Southwestern College

Institutional Technology Department
900 Otay Lakes Rd, Chula Vista, CA 91910
619-421-6700 Ext:4357
helpdesk@swccd.edu