DEPARTMENT OF HUMAN RESOURCES

Office of Employee Relations & Title IX

Video Teleconferencing Meeting
Safeguards and Best Practices

BACKGROUND:

Zoom-bombing or Zoom-raiding, is a form of attack or intrusion into a public video teleconferencing-based virtual meeting. Zoom is the market leader in this technology and is ubiquitously used to describe this form of communication. The intrusions can come in many forms, including pornography, hate speech, threats, sexual harassment, and other inappropriate content.

Since the shift to remote operations in March 2020, the Southwestern Community College District has encountered several instances of intrusions in public video teleconferencing meetings. These intrusions were addressed immediately and handled professionally by the SWC moderators and hosts. However, these intrusions also show the reality and severity of such cyber-attacks on video teleconferencing platforms, and should serve to motivate you to take all necessary precautions to avoid similar attacks in the future.

BEST PRACTICES TO AVOID INTRUSION a.k.a. ZOOM-BOMBING (SWCCD supports Zoom for video teleconferencing, for other video teleconferencing platforms please refer to their security recommendations):

- **Most Importantly - DO NOT GIVE UP CONTROL OF YOUR SCREEN SHARE.** You can set this as a default for all meetings that you schedule, or you can turn it on after a meeting has begun by using the host controls at the bottom. Click the arrow next to the Share Screen and then Advanced Sharing Options. Under "Who can share?" choose "Only Host" and close the window. You can set the lock on the Screen Share by default in your web settings.

- ***Consider using a two-step verification process*** – where you provide a randomly generated Meeting ID when scheduling your event, and require a password to join. You can publicly

announce the meeting and provide the meeting ID, but the password will only be given out via-e-mail or Direct Message.

- ***Avoid using your personal meeting number*** – this is your number and should anybody gain access to your number, they can join any future meeting.

- ***Permission to record must be obtained from all attendees of a Zoom meeting before you initiate recording of the Zoom meeting in question.***

Under Advanced Options, you should:

- ***Enable a waiting room*** - so you can see who you're allowing into the virtual meeting room. In the recent intrusions, there were several fake/prank names identified in the waiting room who were appropriately not allowed to enter.

- ***NOT allow participants to join the meeting before you or the co-host*** – this will eliminate any chance that a hacker can post something inappropriate before you are in control of the room.

- ***Select the option that only one participant can share at the meeting*** – to avoid anybody else from taking control of the screen share feature.

- ***Select the option that only host can share the screen*** – this prohibits participant from sharing their screens and overriding the host.

Under Managing Participants/More, you should:

- ***Mute participants at entry*** – this will ensure that all microphones are off and avoid any potential for intrusions or accidents.

- ***Not allow participants to unmute themselves*** – this will give you control of who you want to hear from and prohibit anybody from interrupting or inserting inappropriate audio.

- ***Not allow participants to rename themselves*** – this will prohibit any participant from changing their profile/creating a new alias for purpose of posting a new, potentially inappropriate profile picture.

- ***Lock the meeting*** - which prohibits anyone from joining the meeting after it begins, even if they are registered, have the meeting ID, and have a password.

Under Basic Settings, you should:

- ***Block ability to chat privately*** – this will prohibit a participant from sending a 1:1 chat to another participant.

- ***Consider turning off the public chat entirely*** – this will prohibit participants from sending a

message that is visible to all participants. There is an option to have participants virtually raise their hand which will put them in a que available to the host.

- ***You should disable annotations and whiteboards*** – this will prohibit any participant from drawing on the shared screen.
-
- ***You should disable allow removed participants to rejoin***- this will ensure removed participants cannot rejoin.

If You Have an Intrusion:

- ***You can/should remove unwanted/disruptive participants*** – mouse over participant's name and several options appear including Remove. Click Remove to kick them out of the meeting. Once removed, they will not be allowed to rejoin, but you have control to let them rejoin if you remove the wrong person.

- ***Acknowledge the Situation*** – let participants know that you believe the meeting has been Zoom-bombed and seek their comfort level in continuing forward with the meeting, having ensured that the offender has been removed.

- ***After the meeting*** – look at your Zoom settings to identify any area of weakness that might have allowed the intrusion to occur.

Reporting an Intrusion to our Office:

Whether the intrusion is into a public meeting or a private meeting, we ask that you gather all of the information you have about the intrusion and provide it to the Office of Employee Relations and Title IX by contacting **Janene McIntyre, Director of Employee Relations and Title IX** at jmcintyre@swccd.edu or **Meng Zhang, Employee Relations & Title IX Coordinator** at mzhang@swccd.edu.

Helpful information for our review includes the meeting title & meeting ID, date, and time of the meeting, participant's names, alleged intruder name(s), if available, nature of the intrusion, and any evidence of intrusion.

You may also report to Zoom directly:

To report an incident that you believe violates Zoom's terms of service, you can do so by theoptions listed below:

- Report a participant during a meeting.

- Report by email, by sending the following information to trust@**zoom**.us. Subject: Violation of Terms of Service. Description: Date of Incident. Meeting ID