HOW *AIRSAFE* HELPS TO ENSURE A SECURE ZOOM LINK.

1. PASSWORD PROTECTED MEETINGS

The simplest way to secure ZOOM, and prevent unwanted attendees and hijacking, is to set a password for ZOOM Sessions. It is the ***AIRSAFE*** policy to set passwords for all individual meetings, user, group, or account level sessions and enforce the use of the 5.0 + client on all in house systems to ensure AES 256 GCM encryption is employed.

As a subscription holder ***AIRSAFE*** has set the account settings to not accept connections that do not comply with the password policies and practices. These settings can only be accessed by the account holder.

2. AUTHENTICATE USERS

When creating a new event ***AIRSAFE*** will invite users to join, if you do not receive an invitation from ***AIRSAFE*** you will not be able to participate. If the user has not been authenticated in the waiting room they will also be denied entry. All ***AIRSAFE*** sessions are at invitation only and all waiting rooms and sessions are monitored.

3. JOIN BEFORE HOST

AIRSAFE does not permit attendees to join before the host. All attendees will be pending authentication in the waiting room before being permitted access to the meeting. This is a system option and cannot be changed by the end user.

4. MEETINGS ARE LOCKED DOWN

Once an ***AIRSAFE*** session has begun, and all attendees are accounted for, the session will be LOCKED. This prevents any other users from joining the meeting without a request to support at ***AIRSAFE***.

5. TURN OFF PARTICIPANT SCREEN SHARING

AIRSAFE does not allow participants to share screen material or files. Inappropriate behavior will result in immediate termination of a users connection. All ***AIRSAFE*** sessions are monitored.

6. USE A RANDOMLY-GENERATED ID

AIRSAFE uses a randomly generated ID for meetings when creating a new event. In addition, these are not shared publicly, they are distributed as part of the invitation.

7. USE WAITING ROOMS

AIRSAFE enforces the use of the “Waiting Room” feature as a way to further screen its participants before they are allowed to enter a meeting. This gives ***AIRSAFE*** greater control over session security.

8. AVOID FILE SHARING

AIRSAFE does not allow file sharing on this platform. All files required for ***AIRSAFE*** courses and meetings are distributed separately from the ZOOM client. Authentication to the ***AIRSAFE*** portal is required for this information to become available.

9. REMOVE NUISANCE ATTENDEES

AIRSAFE will not tolerate inappropriate material or behavior in any of its meetings or ZOOM sessions. If an attendee is found disrupting a meeting, they will be disconnected and disabled. This action will not allow then to rejoin the session without contacting ***AIRSAFE*** support. ***AIRSAFE*** meetings are monitored through out their duration.

10. CHECK FOR UPDATES

AIRSAFE checks for updates to all its software to ensure that potential security issues are patched and all applications have the latest software build.

For further security improvements and information you can refer to;

https://blog.zoom.us/ceo-report-90-days-done-whats-next-for-zoom/