HOW TO SECURE MEETINGS IN BLUEJEANS

Videoconference trolling disrupts online meetings and classes with disturbing language or images through screen sharing. We encourage you to secure your meetings, participants, and data, and recommend the following methods.

Meeting Settings

- **Use a One-Time Meeting ID:** Sharing your Meeting ID on social media or other public forums can lead to uninvited attendees joining your session. Using a One-Time Meeting ID ensures that you will not be exposing your Personal Meeting ID to the public, which could expose your other meetings to more unwanted guests. You can find this setting when you set up the invitation.
- **Use Passcodes:** BlueJeans offers users two types of passcodes: (1) Moderator Passcodes & (2) Participant Passcodes.
    1. Moderator Passcodes require that the meeting host or a delegate enter a code to start the meeting.
    2. Participant Passcodes ensure that only attendees with the correct code can join the meeting.
- **Watch Who Joins the Meeting:** Select an audible alert to announce when an attendee joins and enable entry and exit banners to present the name of the joining attendee. Use the meeting roster to check who is in the videoconference.
- **Master the Controls:** Expel or drop a participant automatically removes that meeting participant and bans them from rejoining the meeting. Lock a meeting once all of the required individuals are present. Control participant audio and video with mute all and participant-specific controls.
- **Leverage Live Meeting Controls for Large Meetings:** Delegate responsibilities to another individual who can access all of the meeting controls.

Other suggestions to secure a meeting

- Do not publish meeting URLs in public communication channels
- Remind participants to not share meeting details