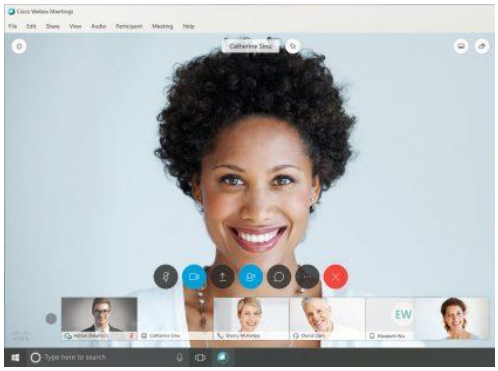
Online Collaboration Tools Guidelines

As you may have seen or heard in recent news, some video conferencing meetings are getting interrupted or hijacked, and inappropriate content has been posted in Zoom meetings (referred to as Zoombombing). Below are some reminders and general guidelines for NJM staff who collaborate online.

Use only approved collaboration tools available to NJM staff:

The following tools are available to support communication remotely:

- **Voice-only conference bridge lines** – These lines can be scheduled as a Resource via Outlook. They are useful when voice-only collaboration is needed without sharing content or using video.
- **Microsoft Skype for Business** – Available for internal-only communications - Instant Messaging, Audio, and Video meetings can be held between several NJM employees simultaneously.
- **Cisco WebEx** – This collaboration suite can be used with both internal and external attendees. Options allow for audio, video, content sharing, or a mix of these capabilities for team collaboration. (Note: only the meeting host requires a WebEx account).



Video conferencing tools such as Zoom are not supported at NJM. However, if you are invited to a Zoom meeting for work-related purposes, such as an invite from a vendor, you are permitted to attend. Please remember not to post or share any sensitive information while on these third-party conferences, as they are currently having privacy and vulnerability issues.

WebEx guidance for securing your video conferencing meetings:

Cisco Webex Meetings provide a secure environment and can be configured as an open space to collaborate. Understanding the security features can allow you to make your Webex meetings more secure.

Best Practices for Hosts: As a host, you are the final decision maker concerning the security settings of your meeting. You control nearly every aspect of the meeting, including when it begins and ends. Below are security best practices to use when scheduling the meeting, which will help keep meetings and information secure.

- Do not share your Audio PIN with anyone.
- Secure your meeting with a complex password, enabled by default.
- Do not reuse passwords for meetings. Scheduling meetings with the same passwords weakens meeting protection considerably.
- Never share sensitive information in your meeting until you are certain who is in attendance.
- Use Entry or Exit Tone or Announce Name Feature, enabled by default, to prevent someone from joining the audio portion of your meeting without your knowledge.
- Whether for work or personal, never share links to remote meetings, conference calls, or virtual classrooms on open websites or open social media profiles.

View additional information about securing your WebEx meetings.