

Guidance for Virtual Meeting Security *(updated 1 October 2025)*

This guidance applies to **CBPO-hosted public, partnership meetings** (i.e., those that appear on our [Meetings Calendar page](#)). The links included below detail options for meeting management in MS Teams. Additional guidance for Zoom/WebEx features is cataloged in Appendix C.

General best practices

1. **Teams is the CBPO-preferred meeting platform.** While CBPO offers WebEx and Zoom in addition to MS Teams, CBPO's Help Desk supports Teams only. Additionally, meetings hosted in one of CBPO's onsite conference rooms should utilize Teams for maximum compatibility with our meeting room A/V equipment.
2. **All meetings should be recorded for internal use only.** Note, **recordings are not to be shared or disseminated** (though, depending on your settings, recordings might be available to meeting participants automatically).
3. **Meeting links/passwords should NOT be published directly on calendar entry.** Instead, place access information in the meeting agenda attached to the entry. Sample text for "Location" field:

For in-person participation, please join us in the CBPO Blue Crab/Oyster Room (106-107) at 1750 Forest Drive Annapolis, MD. To access the meeting via Microsoft Teams, please use the link at the top of the agenda.

4. **Default settings should be used**, as follows, for all meetings (screen shots included in Appendix A):
 - a. [Disable camera and microphone](#) and screen-sharing for all attendees. Teams allows organizers and presenters to [disable the camera and/or mic of all attendees, or of individuals](#), at any time during a meeting. We recommend keeping all attendees' cameras and mics disabled unless they raise their hands to speak.
 - b. *(Optional)* Participants who join the meeting via phone can be allowed to [bypass the lobby](#) and access their mics, as they will be unable to raise their hands or use the chat.
 - c. Disable screen-sharing for all attendees [by managing roles in meeting options](#). To allow screen-sharing by a participant, promote them to

“presenter” during the meeting and return them to the participant role when possible, as presenters cannot utilize the raise hands feature.

- d. [Enable lobby/waiting room](#) (rather than admit all attendees automatically) to review participants prior to admittance.
5. **Secure additional meeting support from a team member by adding as co-organizer or presenter.** This person can help monitor the meeting chat, review participant names for meeting entry, and watch for potential meeting disruptions. This person can also be ready to remove a participant, if necessary.
6. **Communicate the security procedures to meeting attendees.** This can be done in several ways, which are described in Appendix B.

How to handle a disruptive participant/bot

If a meeting is compromised by a bot or bad actor, please take the following steps:

1. **[Remove the participant](#)** as soon as possible and then **[lock the meeting](#)**. *Note: you can continue the existing meeting, but no additional attendees will be able to join, limiting participation. You may also consider ending the meeting and sharing a new link (see 2) if you are expecting additional participants to join.*
2. (Optional) **[End the meeting](#)** and share a new meeting link/password with attendees. *Note: this will limit public participation.*
3. **Report the incident** to the meeting platform and CBPO’s Admin Team (R3_CBPO-Admin_Team@epa.gov) and Help Desk (helpdesk@chesapeakebay.net).
4. **Change future instance of Meeting URLs if meeting is recurring.**

Troubleshooting issues

1. If **participants cannot unmute or enable their camera** after being given permission, advise them to leave the meeting and rejoin. Joining the meeting via browser (instead of the Teams app) may also alleviate this issue.

Appendix A: Default meeting options

Meeting access

Who can bypass the lobby?

Even if Everyone is selected, your org policy may require certain participants wait in the lobby until a member of your org or a trusted org joins. This could include people joining without an account, people from untrusted orgs, and people dialing in.

People in my org and guests



People dialing in can bypass the lobby



Who can admit from the lobby

Organizers and co-organizers



Announce when people dialing in join or leave



Roles

Choose co-organizers:

Has the same capabilities as the organizer.

Search for participants



Who can present

Only organizers and co-organizers



Enable language interpretation



Add interpreters who can interpret one language into another in real-time. To assign interpreters, send the meeting invite then refresh this page and choose them.

Participation

Allow mic for attendees

Turn this off to prevent attendees from unmuting. You can allow them to unmute individually as needed.



Allow camera for attendees

Turn this off to prevent attendees from sharing video. You can allow them to share video individually as needed.



Meeting chat

On



Q&A

Organizers can customize Q&A to allow anonymous posts, review questions before publishing, and more. [Learn about Q&A.](#)



Allow reactions



Allow attendance report



Recording & transcription

Record and transcribe automatically

This will also turn on transcription.



Spoken language in this meeting

Language that everyone is speaking in this meeting. This setting affects all participants. To use it, select the correct spoken language before the meeting starts.

English (US)



Appendix B: Communication Examples

Communication of the new security protocols will ensure that meeting attendees and participants can participate fully in virtual/hybrid meetings and know what to expect if a meeting is compromised. Below are some recommendations and sample text for communication.

1. **Address the security procedures verbally at the beginning of the meeting.** This may only be necessary for the first few meetings of a group.

Sample statement

Due to recent instances of online intruders in public partnership meetings, we are now implementing some stronger security protocols. In particular:

- *Meeting participants will now join with their cameras and microphones off. If you wish to speak, please raise your hand, and we will give you microphone access. You will then be able to mute/unmute as you normally would for the rest of the call, so please continue to be mindful of your microphone.*
- *Presenters/WG Leadership will be given normal microphone, camera, and screenshare access for the duration of the call.*
- *We will collect votes via chat for decisional items where we need to go member by member, and anyone who wishes to ask questions or register a comment should use the raise hand feature.*
- *Meeting links will no longer be available in the "location" field on the website calendar pages, so please refer to agendas or calendar invitations for meeting information.*
- *If there is an unwanted intruder on the call, we will do our best to remove the participant as quickly as possible and lock or end the meeting. If the meeting is ended, we will then share a new meeting link with those on the distribution list.*

Thank you in advance for your flexibility as we adapt to these new procedures. We welcome your feedback on any impacts to your meeting participation.

2. **Include statement regarding security procedures in chat (pin comment) and/or in the meeting agenda.**

Sample text

Please note we will be using enhanced security settings for CBP meetings moving forward. You will begin with your cameras and mics off. If you would like to speak,

please raise your hand, and I will grant you your normal access to cameras and mics, which will remain for the rest of the meeting. Thank you for your patience!

3. Email participants in advance of meeting with new security procedures.

Sample email

Please read the following information regarding meeting security procedures:

All meeting attendees' cameras and microphones will be muted at the start of the meeting.

To request access to the microphone and camera, meeting participants should use the raised hand feature on Teams. Once access has been granted by the meeting organizer, can then unmute your mic and turn on your camera. Unless instructed otherwise, once a participant has microphone or camera access, they will have this permission for the remainder of the meeting.

Access to chat will be provided. Should it be necessary, the Q&A feature on Teams will be utilized to field participant questions.

Compromised Meeting Plan:

If the meeting is interrupted by an intruder, the meeting staffer and coordinator will remove the participant and lock the meeting, disallowing any new attendees. It may also be necessary to provide attendees with a new meeting link, which will be shared via email to meeting participants. Please do NOT share this information publicly or post it to the Chesapeakebay.net webpage.

Appendix C: Detailed information by platform

How to:	Teams	Zoom	Webex
Join meetings via app, browser, and phone	Teams meeting access instructions	Zoom meeting access instructions	Webex meeting access instructions
Join a meeting via mobile	Teams mobile instructions	Zoom mobile instructions	Webex mobile instructions
Control meetings as a host/meeting organizer/presenter	Teams meeting control instructions Teams meeting mute/unmute participant instructions	Zoom meeting control instructions Zoom meeting mute/unmute participant instructions	Webex meeting control instructions Webex meeting mute/unmute participant instructions
Manage security features in the account or meeting settings	Team meeting control instructions	Zoom account security controls instructions	Webex account security controls instructions
Manage in-meeting security features as a host	Teams in-meeting security feature instructions	Zoom in-meeting security feature instructions	Webex in-meeting security feature instructions
Manage recordings	Teams recording settings instructions Teams recording management	Zoom recording setting instructions Zoom recording management	Webex recording setting instructions Webex record management instructions

	and distribution instructions	and distribution instructions	Webex record distribution instructions
How to:	Teams	Zoom	Webex
Managing lobbies/waiting/rooms	Teams lobby management instructions	Zoom waiting room settings instructions Zoom waiting room in-meeting management instructions	Webex lobby settings instructions Webex lobby management instructions
Add a co-organizer/co-host	Teams co-organizer assignment instructions	Zoom co-host assignment instructions	Webex co-host assignment instructions
Use the meeting participant features	Teams meeting participant features	Zoom meeting participant features	Webex meeting participant features
Activating and accessing the transcription feature	Teams live transcription feature	Zoom audio transcription instructions	Webex meeting transcription instructions