VIDEO CONFERENCING BEST PRACTICES

For Webex and Zoom

A large population of Illinois has transitioned to working from home for the time being. With this unprecedented move to remote work, many are using video conferencing for the first time for business, school, and for social connectivity. The Department of Innovation & Technology (DoIT) has seen numerous stories and accounts regarding cyber threats related to various video-teleconferencing solutions. Reports range from conferences being accidentally disrupted to some maliciously interrupted in order to transmit hate speech, profanity or even pornographic material.

Remember there is a learning curve with any new technology. This includes how to use it effectively and securely. Here are some simple recommendations and best practices to use the video conferencing in a more secure manner.

Webex Best Practices

- Webex is the standard video conferencing software for conducting state business for State of Illinois employees supported by DoIT. (Please see Zoom tips below as well)
- As with any technology, follow your organization's guidelines for sharing sensitive data. If in doubt, don't share.
- Auto Lock your Personal Room for secure meetings. This prevents all attendees in your Webex lobby from automatically joining in the meeting. The host will see a notification when attendees are waiting in the lobby and will authorize the attendees to join. This can be done from My Webex > Preferences > My Personal Room on your Webex site.
- Schedule a meeting instead of using your Personal Room.
    - Personal Rooms web links do not change.
    - Improve security by scheduling a meeting which includes a one-time web link.
- Scheduled Meetings are unlisted by default by the State Administrator for all Webex sites.
    - "Unlisting" Meetings enhances security by requiring the host to inform the meeting attendees, either by sending a link in an email invitation, or hosts can enter the meeting number using the Join Meetings page.
    - "Listing" a meeting publicly exposes meeting titles and meeting information publicly.
- If using your Webex Personal room, set your Personal Room notifications before a meeting to receive an email notification when attendees are waiting for a meeting to begin. You will then be able to review the participant list and expel any unauthorized attendees.
- Think about setting up a password for every meeting by creating a high-complexity, non-trivial password (strong password).

    - A strong password should include a mix of uppercase and lowercase letters, numbers and special characters (for example, $Ta0qedOx!).
    - Passwords protect against unauthorized attendance since only users with access to the password will be able to join the meeting.
    - Do not reuse passwords for meetings.
- As the host, you have the ability to use an entry or exit tone or “Announce Name” feature to prevent someone from joining the audio portion of your meeting without your knowledge.
    - This feature is enabled by default for Webex Meetings. For notifications, select Audio Conference Settings > Entry and exit tone > Beep or Announce Name. Otherwise, select No Tone.
- Do not allow attendees or panelists to join before host.
- Assign an alternate host to start and control the meeting.
    - This keeps meetings more secure by eliminating the possibility that the host role will be assigned to an unexpected, or unauthorized, attendee or in case of a lost connection to your meeting or conflicting meetings.
    - One or more alternate hosts can be chosen when scheduling a meeting.
    - An alternate host can start the meeting and act as the host. The alternate host must have a user account on the Webex Meetings website.
- Hosts can:
    - Lock the meeting once all attendees have joined the meeting. This will prevent additional attendees from joining. Hosts can lock/unlock the meeting at any time while the session is in progress.
    - Expel attendees at any time during a meeting. Select the name of the attendee whom you want to remove, then select Participant > Expel.
    - Set passwords for recordings before sharing them to keep the recording secure. Password-protected recordings require recipients to have the password in order to view them. Send the password in a separate email.
    - Create a Host Audio PIN. Your PIN is the last level of protection for prevention of unauthorized access to your personal conferencing account. Should a person gain unauthorized access to the host access code for a Personal Conference Meeting (PCN Meeting), the conference cannot be started without the Audio PIN. Protect your Audio PIN and do not share it.

ZOOM Best Practices

- While Webex is the videoconferencing/teleconferencing standard for agencies, boards and commissions supported by DoIT, Zoom is often used by vendors and other organizations state employees conduct business with. Zoom is also a popular platform for personal and educational use as well.
- As with any technology, follow your organization’s guidelines for sharing sensitive data. If in doubt, don’t share.

- Don't make meetings or classes public. You can require participants to use a password, or the meeting manager can make participants first appear in the waiting room and be admitted individually.
- Invite with care. Do not share links to your meeting on social media. Email or text them directly to participants.
- UPDATES are important to decrease security risks! Make sure participants have the latest version of Zoom's software, which was updated in January 2020. The January update added meeting passwords by default and disabled a feature allowing users to randomly scan for meetings to join. This update took care of one of the issues seen in the news frequently as these users were most**ly** likely using older versions of the software. UPDATE your software and operating systems regularly!
- As the Host, you can:
    - Limit screen sharing. Hosts can prevent others from posting video by changing the screen sharing options to "Host Only."
    - Lock the door. You can close your meeting to newcomers once everyone has arrived. Hosts can click the Participants tab at the bottom of the Zoom window to get a pop-up menu, then choose the Lock Meeting option.
    - Use a silencing feature. You can disable video for participants and mute an individual or all attendees.
    - Disable the ability to text/chat during the session to prevent the delivery of unwanted messages.
    - Kickout uninvited guests. Hosts can remove a participant by putting the mouse over that name and choosing the "Remove" option. You can block people from rejoining meetings if they were removed.

With any technology, you must always update and patch your software and operating systems. Why? Because vulnerabilities and "bugs" are found every day in software and operating systems, but professionals are constantly working to fix them. These "fixes" come in the form of updates and patches to software and operating systems. If you don't update your software and operating systems, you are not fixing any of the problems that have been discovered.