Virtual Meeting Best Practices/Guidebook

PURPOSE: To provide clear and simple guidelines and tips for running secure virtual meetings with the following tools.

- GoToWebinar
- Cisco WebEx
- Microsoft Teams
- Zoom

GENERAL FEATURES:

- See attachment A for a list of general features by tool
- See attachment B for an Infographic from the National Institute of Standards and Technology

SPECIFIC TOOLS

CISCO WebEx (Spark) - Admin Settings

Make All Meetings Unlisted

- Require Passwords for all Meetings, Events, and Sessions
- Enforce Meeting Password When Joining from Phone or Video Conferencing Systems
- Require Sign-In When Joining a Meeting, Event, or Training Session
- Do Not Allow Join Before Host
- Enforce Personal Room Locking After a Default Time
- Restrict Unauthenticated Users
- Account Management

For specific Admin instructions go to: https://help.webex.com/en-us/ov50hy/Cisco-Webex-Best-Practices-for-Secure-Meetings-Control-Hub#task_EF159729746DEDC092181B2BC1F44682

CISCO WebEx (Spark) – End User Settings

- Using Your Personal Room
  - Auto Lock Personal Room
  - Personal Room Notifications Before a Meeting
  - Personal Room Notifications During a Meeting – Allows you to screen who wants to join the meeting
- Scheduling the Meeting
  - Schedule Unlisted Meetings in Classic View
  - Choose the Meeting Topic Carefully
  - Secure meetings with a complex password
  - Exclude Meeting Password from Invitations
  - Require Attendees to Have an Account on Your Site
  - U se Entry or Exit Tone or Announce Name Feature
  - Request That Invitations Are Not Forwarded
  - Assign an Alternate Host

- During the Meeting
  - Restrict Access to the Meeting (lock the meeting once you start so no one else can join)
  - Validate Identity of All Users in a Call
  - Remove a Participant from the Meeting
  - Share Application not the Screen
- After the Meeting
  - Assign Passwords to Recordings
  - Delete Recordings
- Personal Conferencing for Hosts
  - Create a strong Audio PIN and protect it.

For specific directions go to: https://help.webex.com/en-us/8zi8tq/Cisco-Webex-Best-Practices-for-Secure-Meetings-Hosts

GoToMeetings

- Secure Content Sharing: Within the content sharing and security preferences users can choose what content to share, with whom, and how long to make it available for viewing.
- Meeting Lock and Password Protected Meetings: With features like meeting lock, you can keep uninvited guests out of a meeting. With password protected meetings, only those with the code will be able to gain entry, which helps keep your meeting secure from others who may know your personal meeting code.
- GoToMeeting Security Compliance Features: All tiers of GoToMeeting include security features such as Secure Socket Layer Encryption, AES-256 Bit Encryption, a SOC2 Certified Data Center, Rich Based Authentication and HIPAA readiness.
- Set content sharing and security to: Only myself and people I choose
- Helpful Reading: COVID-19: Tips for Staying Secure Using GoToMeeting: https://support.goto.com/gotomeeting/help/covid-19-tips-for-staying-secure-using-gotomeeting

MS Teams

- Admin settings
  - Here you can turn on or turn off file sharing and cloud file storage options.
- Key Roles
  - **Organizer** The user who creates a meeting, whether impromptu or by scheduling. An organizer must be an authenticated in-tenant user and has control over all end-user aspects of a meeting.
  - **Presenter** A user who is authorized to present information at a meeting, using whatever media is supported. A meeting organizer is by definition also a presenter and determines who else can be a presenter. An organizer can make this determination when a meeting is scheduled or while the meeting is under way.
  - **Attendee** A user who has been invited to attend a meeting but who is not authorized to act as a presenter.
- **Structured meetings** (where Presenters can do about anything that should be done, and attendees have a controlled experience). After joining a structured meeting, presenters control what attendees can do in the meeting.

Actions	Presenters	Attendees
Speak and share their video	Y	Y
Participate in meeting chat	Y	Y

Actions	Presenters	Attendees
Change settings in meeting options	Y	N
Mute other participants	Y	N
Remove other participants	Y	N
Share content	Y	N
Admit other participants from the lobby	Y	N
Make other participants presenters or attendees	Y	N
Start or stop recording	Y	N
Take control when another participant shares a PowerPoint	Y	N

Helpful Reading: https://docs.microsoft.com/en-us/microsoftteams/teams-security-guide
Advanced Reading: https://docs.microsoft.com/en-us/microsoftteams/meeting-settings-in-teams

Zoom

Security Protocols
Don't publicize Zoom classroom meetings on social media or public forums
Set a password for all meetings
Turn off file transfer
Keep the Zoom application updated to the most recent version
Don't use a Personal Meeting ID (PMI) to host a classroom or large event meeting
Disable private chat
Allow chat with host only
Set "Screen Sharing" to "Host Only"
"Lock Meeting" after all participants have joined
Turn off annotation when not needed
Use "Waiting Room"

- Zoom users should not make meetings on the site public
- Zoom videos are not recorded by default, but call hosts can choose to record them and save to Zoom servers or their own computers without participants' consent, though participants do receive a notification when a host starts to record
- Helpful Videos
  - https://www.msn.com/en-gb/money/technology/zoom-101-securing-your-meetings-virtual-classrooms/vi-BB1288Zv (excellent video)
  - https://www.wordfence.com/blog/2020/04/safety-and-security-while-video-conferencing/
- Advanced Security Reading –
  - https://zoom.us/docs/doc/Zoom-Security-White-Paper.pdf
  - https://blog.zoom.us/wordpress/2020/03/20/keep-uninvited-guests-out-of-your-zoom-event/

Attachment A – Feature Comparison

Feature	GoTo	Cisco	Microsoft Teams	Zoom
Private Messaging	Y	Y	Y	Y
Group Messaging	Y	Y	Y	Y
VoIP	Y	Y	Y	Y
PSTN Conference Dial-in*	Y	Y	Y	Y
Video Conferencing	Y	Y	Y	Y
File Sharing	Y	Y	Y	Y
Screen Sharing	Y	Y	Y	Y
Video Tiles	25 (meeting) 6 (webinar)	6 (but you can scroll through to see more)	9 (as of May 1)	49
Recording	Y	Y	Y	Y
Attendees (with audio)	1000	3000	250	100 – 500 depending on license

*Note - Toll Free Numbers: Generally, you can add a toll-free number to the service, but that will be an extra per minute per attendee cost back to the organization.

Attachment B

Resources:

- NIST
- Zoom Rushes Patches for Zero-Day Vulnerabilities
- How to avoid becoming a victim of 'zoom bombing'
- Twitter Article on Zoom
- https://www.northstarmeetingsgroup.com/Planning-Tips-and-Trends/Event-Planning/Event-Technology/Coronavirus-Checklist-Changing-In-Person-Event-Virtual-Meeting
- A special thank you to Michigan Association of Counties for some of the general tips!