BEST PRACTICES FOR ZOOM MEETINGS
(USING THE ZOOM WEB PORTAL – TENNESSEE.ZOOM.US)

Recommended Settings for Secure Sessions/Meetings (please keep in mind that not all sessions/meetings are the same so what works for a smaller session might not work for a larger session)

- Make sure you are always using the latest Zoom client.
  - Open the client; click your picture; click Check for Updates.
  - Version 5.5.2 (12494.0204) is the latest version, released February 8, 2021.
- When scheduling your class or meeting, use these recommended options when possible:
  - Meeting ID
    - Choose Generate Automatically
    - Never use your Personal Meeting ID
  - Security
    - Check Passcode
      - Never share your class session or meeting links on social media or other public sites.
    - Check Waiting Room
      - This will allow the host to decide who enters the Zoom meeting.
      - Faculty members may need to collaborate to find the best way to host large classes.
  - Video
    - Host - On
    - Participants - Off
  - Meeting Options
    - Uncheck Enable join before host
    - Check Mute participants upon entry
    - Check Only authenticated users can join (unless you have a guest speaker from outside the University)
    - Name at least one Alternative Host
      - This will allow someone to keep an eye on activity while you teach or lead the meeting.
      - This will also allow them log in as host if you are late or unavailable.
      - If you do not name someone here, you can add them as a co-host when you log in before the start of the meeting.
  - Save
More Settings (Go to Settings on the left)

• Security
  o Waiting Room
    - This is not an all-or-none option, as you can “Edit Options” based circumstances, such as the size of your class or meeting.
    - “Everyone” is a good choice if it is a smaller meeting or class.
    - “Users not in your account”
    - “Users who are not in your account and not part of the allowed domains”
  o Require a passcode when scheduling new meetings – toggle on
  o Require a passcode for participants joining by phone – toggle on
  o Only authenticated users can join meetings
    - Use this when all participants should have a UT login.
    - This may become an automatic setting in the near future.
  o If your class is not offered to students living in another county countries, or if you know in exactly which countries your students/participants are living, this is a great option to turn on.
    - Toggle on, then choose Only allow users from selected countries/regions.
    - This will help if someone is using a spoofed IP address that appears to be coming from a country when you know you have students there.
  o Host video – toggle on
  o Participants video – toggle off
  o Allow participants to join before host – toggle off
  o User Personal Meeting ID (PMI) when scheduling a meeting – toggle off
  o Mute all participants when they join a meeting – toggle on

• In Meeting (Basic)
  o Private chat – toggle off
  o File transfer – toggle off
  o Feedback to Zoom – toggle off
  o Co-host – toggle on
    - This will allow the host to add a co-host during the meeting.
    - Will allow someone with the hosts permission to share their screen.
    - Co-hosts have the same in-meeting controls as the host.
    - Be cautious not to make them “host” as that will transfer all control to that other person.
  o Screen sharing – toggle on
    - Who can share? Click Host Only
    - As long as Host Only is checked, no one else can share unless the host allows them to.
  o Annotation – toggle off
  o Whiteboard – toggle off
  o Allow participants to rename themselves – toggle off
These settings are incredibly important to know about and remember if needed during a Zoom session.

- Share Screen (click the ^)
  - Advanced Sharing Options
    - How many participants can share at the same time?
      - Click Only one can share at a time
    - Who can share?
      - Click Only Host

- Chat
  - Click Chat, then click on the “…” for More at the bottom of the Chat window (across from “Everyone”)
  - Choose Everyone Publicly from the options and do not allow private chats

- Security
  - Unmute themselves
    - This requires them to raise their hand or tell them which reaction to use so only the host and co-host can unmute.
    - If you plan to have a lot of discussion, leave this checked and you can mute those individuals who need to be temporarily muted.
  - Lock Meeting
    - Only after allowing everyone in first
    - Anyone who is late will not be able to enter
    - Anyone who is inadvertently bumped cannot re-enter
    - May want to save this for when you have to remove participants, then Lock Meeting

- To remove meeting participants mouse over that participant’s name and choose “Remove” from the options.

What to do after the Zoombombing

Your session was compromised so you must take the following action as quickly as possible:

1. Notify Sandy Lindsey, UTIA CISO, by emailing sandy@tennessee.edu, and copy Angela Gibson, UTIA CIO, at gibsonaa@tennessee.edu. In the email, please include the following information:
   - Meeting ID
   - Class and time of class (or meeting and time of meeting)
   - Class roll, including email addresses of students (or list of meeting invitees)
   - Description of what happened
Sandy will inform those who need to know, including UTK’s Zoom administrator, UTK CISO, and UTK CIO. Please call Sandy at (865) 806-5224, if you have questions during this process.

2. Call UTPD at (865) 974-1092, to report this crime.
   - Law enforcement must be contacted by the person involved, ideally the professor or host.
- UTPD will ask you for some of the same information you have given to me, but I will be working with OIT to get Zoom reports started.
- UTPD may do the full investigation, or may turn it over to other law enforcement based on the details of what happened.