CISA
CYBER+INFRASTRUCTURE

TIPS FOR VIDEO CONFERENCING

TIP 1: ONLY USE APPROVED TOOLS

Only use organization-approved software and tools for business, including company-provided or -approved video conferencing and collaboration tools to initiate and schedule meetings.

1. **Don't install unapproved clients.** When joining meetings initiated by third parties that use collaboration tools not approved by your organization, do not attempt to install software—join web (browser) based session instead. Do not use work email addresses to sign up for unauthorized/free tools.

2. **Ensure links are correct.** If logging into a collaboration tool via a web browser, be careful to accurately type the domain name of the website. Be wary of links sent by unfamiliar addresses, and never click on a link to a meeting sent by a suspicious sender. Verify that meeting links sent via email are valid.

TIP 2: SECURE YOUR MEETING

Tailor security precautions to be appropriate for the intended audience. Plan for what to do if a public meeting is disrupted. Take precautions to ensure your meeting is only attended by intended individuals.

1. **Consider attendees.** Do not make meetings "public" unless they are intended to be open to anyone. For meetings that will be broadly attended, ensure you have the capability to mute all attendees and limit the ability of attendees to share screens.

2. **Have a plan to terminate a meeting.** Particularly when conducting meetings with a large audience, have a preestablished plan that details:

   a. The circumstances in which a meeting will be terminated if it is disrupted,

   b. Who has the authority to make that decision, and

   c. How the meeting termination will be executed.

3. **Secure private meetings.** For private meetings, require a meeting password and use features such as a waiting room to control the admittance of guests. For enhanced security, use randomly generated meeting codes and strong passwords and do not reuse them. Do not share a link to a teleconference on an unrestricted, publicly available social media post. If possible, disable allowing participants to join a meeting before the host and automatically mute participants upon entry.

4 **Control attendees.** Provide the link to the meeting directly to specific people and share passwords in a separate email. If possible, require unique participant credentials, monitor meeting members as they join, and lock an event once all desired members have joined. Utilize features to permit removal of any meeting guest during the course of the meeting.

TIP 3: SECURE YOUR INFORMATION

Tailor your security precautions appropriate to the sensitivity of your data. Only share data necessary to accomplish the goals of your meeting.

1 **Manage screensharing, recording, and file sharing options.** Consider saving locally versus in the cloud based on the specific circumstances (e.g., need to share the recording with a wide audience or the public, using company-issued equipment versus personal equipment). Change default file names when saving recordings. Make sure to consult with your organization's counsel about laws applicable to recording videoconferences and sharing materials through them. Set participant expectations on session recording, screen recording, and screen shots.

2 **Protect sensitive information.** Consider sensitivity of data before exposing it (via screen share or upload) to video conference and collaboration platforms. When sharing a screen, ensure only information that needs to be shared is visible; close or minimize all other windows. If displaying content from organizational intranet sites in public meetings, hide the address bar from participants before displaying the content. Use common sense—do not discuss content you would not discuss over regular telephone lines. When having sensitive discussions, use all available security measures (e.g., waiting rooms and strong passwords), ensure all attendees of the meeting have a need to know, and make attendees aware of expectations for session security.

TIP 4: SECURE YOURSELF

Take precautions to avoid unintentionally revealing information. Ensure home networks are secured.

1 **Don't reveal information unintentionally.** Ensure that your visual and audio surroundings are secure and do not reveal any unwanted information (e.g.; confirm that whiteboards and other items on the wall are cleared of sensitive or personal information, confirm that roommates or family members are not having sensitive conversations in the background). If available, make use of background replacement or blurring options in the collaboration tool.

2 **Consider your surroundings.** Move, mute, or disable virtual assistants and home security cameras to avoid inadvertently recording sensitive information. Do not have sensitive discussions with potential eavesdroppers in your workspace or in a public area. Consider using headphones.

3 **Check and update your home network.** Change default settings and use complex passwords for your broadband router and Wi-Fi network and only share this information with people you trust. Choose a generic name for your home Wi-Fi network, to avoid identifying who it belongs to or the equipment manufacturer. Update router software and ensure your Wi-Fi is encrypted with current protocols (such as WPA2 or WPA3), and confirm that legacy protocols such as WEP and WPA are disabled.

For more information, please visit cisa.gov/telework.