CITE
CENTER FOR INFORMATION
TECHNOLOGY EXCELLENCE

The following guidance is provided by PVAMU to help ensure faculty and staff are equipped to better secure themselves and their use of video conferencing tools.

Telecommuting Guidance for Faculty & Staff

Video Conferencing

- Only use PVAMU approved software & tools to host, initiate and schedule meetings.
- Do not make meetings "public" unless they are intended to be open to anyone.
- Meeting access codes should only be reused for recurring meetings that include waiting rooms or authentication.
- For meetings & lessons, require a password. Provide the meeting link & password in separate emails to participants.
- Manage screen sharing, recording and file sharing options to avoid unwanted or unexpected images.
- Do not share passwords with anyone.
- Be wary of links sent by unfamiliar addresses & verify that meeting links sent by email are valid.
- Make sure everyone knows if a session is being recorded.

Protecting Sensitive Data/Information

- Consider the sensitivity of data before exposing it (via screen share or upload) to video conferences.
- When sharing a screen, ensure only information that needs to be shared is visible.
- Use common sense - do not discuss content you would not discuss over the telephone.
- When having sensitive discussions, ensure all attendees are the intended participants.
- Ensure your visual & audio surroundings are secure.
- Confirm that roommates or family are not within earshot of sensitive conversations.
- Consider using headphones to avoid eavesdroppers.
- Use backgrounds or blur options in video calls/meetings.
- Turn off home security cameras & virtual assistants to avoid inadvertently recording sensitive information.

Securing a Personal Device/Environment

If using a personal device for work from home:

- Require a strong password to log into the device.
- Close all other, non-work related windows & applications before and while using the personal equipment for work.
- Keep the operating systems & all relevant applications up-to-date, & fully patched.
- Turn on automatic patching & run antivirus software.
- Check & update your home network.
- Change default network settings & use complex passwords.
- Change the generic name for your home Wi-Fi network to avoid identifying who it belongs to or the equipment manufacturer.