Advisory on Safe Video-Conferencing

The need for security guidelines for video conferencing is growing as more and more companies look for new and innovative ways to make employees even more productive through video collaboration which has overtaken the traditional face to face meeting. In view of COVID-19, an increasing number of employees is working from home, collaborating with internal teams or customers via video conference on mobile devices including laptop, cellphone, tab etc.

It is important that users of videoconferencing, particularly those that are connecting their own devices to the system, clearly understand their responsibilities when it comes to security. Requisite security policy would provide a set of guidelines for employees working from their personal devices and clear consequences for improper use.

List of Safety Precautions about Video Conferencing:

1. **Create a Bring-Your-Own-Device (BYOD) Policy**
   Always use their own personal devices or else the company's security could be at risk from unsecure networks, lost devices, forgotten or even complete lack of secure passwords.
2. **Keep your conferencing software patched and up-to-date.**
   Purchase Licensed Software with a limited number of participants.
3. **Implement Staff Training**
   Implement adequate training for staff on necessary security measures, particularly when sensitive data and private information is being shared.
   Create and enforce appropriate standard operating procedures (SOPs) with device support.
4. **Review & Update Video Systems**
   Review and enable appropriate security and privacy settings to prevent threat actors from exploiting known vulnerabilities.
5. **Secure Networks or Devices**
   Transmitting sensitive information and data across internal and external networks, businesses/organizations need to be assured that their conferencing solution is safe and not susceptible to security breaches. Make sure users and devices that are accessing the corporate network on-premise or off-premise can be identified and allowed connectivity only if they are authorized and meet company policy.
6. **Check the Signs**
   Video conferencing systems use single sign-on (SSO) for user authentication which greatly reduces the risk of user credentials being lost, stolen or compromised.

Meeting Lock
Once invited attendees have joined, lock the meeting to keep out unknown attendees.

8. **password for enhanced privacy**
Meeting IDs can be guessed, allowing unauthorized attendees to join even if they have not received an invite.

9. **Check Meeting Links**
When you receive a meeting invitation, verify that it is from a known, trusted sender. Also, check the meeting link before clicking, watching out for malicious links with ".exe,"

10. **Report Suspicious Activity**
    - Report to your organizer if any suspicious activity occurred during Conferencing.
    - If you are using an external video conferencing, reach out to the vendor for the best way to report suspicious activities

11. **Protect video conference units with permissions**
Create different access levels for different types of conference, to have control over who can access what.

12. **Have a Video Conferencing Policy in Place:**

A few guidelines most video conferencing policies include are:

- Users must get permission to record a video conference from everyone on the call.
- Personal mobile devices should not be used to record video conferences.
- Sensitive information should be discussed in designated video conference rooms and not in public places or open office spaces.
- Video conferences conducted at a user's desk should train the camera to focus on the users face, and any visible confidential data should be removed from camera view.
- Cameras and microphones should be turned off when not in use.
- Remote control of cameras is for authenticated users only.
- Recording of the video should be notified to the host of the meeting. This should be supported by the application itself.

13. **The Chairperson joins first**
The Chairperson or host of the conference should control admittance.