ITEC-1220-G: Guidance for Secure Video Conferencing

Issue Date: 6/15/2021
Effective Date: 6/15/2021
Online: https://ebit.ks.gov/itec/resources/policies/itec-1220-g-guidance-for-secure-video-conferencing

PURPOSE

To serve as a recommendation to state entities and establish guidelines with cybersecurity principles and practices that individuals and organizations can follow to video conference more securely. Although these guidelines are providing this general risk advisory guidance, individuals and organizations are responsible for their own risk assessments of specific systems and software. For optimum risk mitigation, organizations should implement measures at both the organizational and user levels.

BACKGROUND

The State of Kansas, local and federal government partners, the private sector, and general public have pivoted to widescale remote work and online collaboration. Video conferencing has emerged as a pervasive tool for business continuity and sustained social connection. Although increased telework and online collaboration tools provide necessary capabilities, video conferencing has increased the attack surface exploited by malicious actors.

Once niche products, many of these tools were meant for a subset of the business community and were not scaled for crisis-driven ubiquity. Entire industries, sectors, and stakeholder sets are now profoundly dependent on online tools—simultaneously. Amid the unanticipated exponential growth and unprecedented popularity of these platforms, many video conferencing users have not implemented necessary security precautions—or might be unaware of the latent risks and vulnerabilities.

FOUR PRINCIPLES TO SECURE VIDEO CONFERENCING

CONNECT SECURELY

Risk: The initial settings for home and public Wi-Fi networks and many video conferencing tools are not secure by default, which—if not changed—can allow malicious actors to compromise sensitive data while you work from home.

Mitigation: Change default passwords for your router and Wi-Fi network. Check that you are using Wi-Fi encrypted with WPA2 or WPA3. Verify your video conferencing security settings and use encrypted video conferencing tools whenever possible.

Tips: Here are some simple actionable tips for connecting securely at home.

- Do not connect to video conferencing or collaboration tools when on insecure internet connections or in a public space.
- Change default password to strong, complex passwords for your router and Wi-Fi network.
- Choose a generic name for your home Wi-Fi network to help mask who the network belongs to, or its equipment manufacturer.
- Ensure your home router is configured to use WPA2 or WPA3 wireless encryption standard at the minimum, and that legacy protocols such as WEP and WPA are disabled.
- Avoid using public hotspots and networks.
- Only use video conferencing tools approved by your organization for business use.
- Enable security and encryption settings on video conferencing tools; these features are not always enabled by default.
- Ensure that video streaming and collaboration data is not routed through servers outside of the United States.

CONTROL ACCESS

Risk: Uncontrolled access to conversations may result in disruption or compromise of your conversations, and exposure of sensitive information.

Mitigation: Check your tool's security and privacy settings. Enable features that allow you to control who can access your video chats and conference calls. When sharing invitations to calls, ensure that you are only inviting the intended attendees.

Tips: Here are some simple actionable tips to help control access to your conversations.

- Require an access code or password to enter the event. Try not to repeat codes or passwords.
- Manage policies to ensure only members from your organization or desired group can attend. Be cautious of widely disseminating invitations.
- Enable "waiting room" features to see and vet attendees attempting to access your event before granting access.
- Lock the event once all intended attendees have joined.
- Ensure that you can manually admit and remove attendees (and know how to expeditiously remove unwanted attendees) if opening the event to the public. Be mindful of how (and to whom) you disseminate invitation links.

MANAGE FILE AND SCREEN SHARING AND RECORDINGS

Risk: Mismanaged file sharing, screen sharing, and meeting recording can result in unauthorized access to sensitive information. Uncontrolled file sharing can inadvertently lead to users executing and clicking malicious files and links, which could, in turn, lead to system compromise.

Mitigation: Disable or limit screen and file sharing to ensure only trusted sources have the capability to share. Users should be aware of sharing individual applications versus full screens.

Tips: Here are some simple tips for controlling file and screen sharing.

- Toggle settings to limit the types of files that can be shared (e.g., not allowing .exe files).
- When recording meetings, make sure participants are aware and that the meeting owner knows how to access and secure the recording. Consider saving locally rather than in the cloud. Change default file names when saving recordings. Consult with your organizational or in-house counsel regarding laws applicable to recording video conferences.
- Ensure that recordings and documents are not stored at a location outside of the United States. State of Kansas data should reside within the United States.
- Do not allow other to record meetings without your approval.
- Consider sensitivity of data before exposing it via screen share or uploading it during video conferences. Do not discuss information that you would not discuss over regular telephone lines.

UPDATE TO LATEST VERSIONS OF APPLICATIONS

Risk: Outdated or unpatched video conference applications can expose security flaws for hackers to exploit, resulting in a disruption of meeting privacy and potential loss of information.

Mitigation: Ensure all video conferencing tools, on desktops and mobile devices, are updated to the latest versions. Enable or opt-in to automatic update features, or else establish routine updates (e.g., once weekly) to check for new versions and patch security vulnerabilities.

Tips: Here are some helpful tips to keep applications updated and secure.

- Do not use the free license version of video conferencing or collaboration tools to host meetings.
- Enable automatic updates to keep software up to date.
- Develop and follow a patch management policy across the organization that requires frequent and continual application patching.

- Use patch management software to handle and track patching for your organization.

SECURITY SETTINGS OF COMMON VIDEO CONFERENCING TOOLS

Security Settings Information

In addition to the guidance above, KISO recommends that organization administrators and individual users become familiar with the security settings and capabilities of their preferred video conferencing platform(s). Listed below are links from several popular video conferencing user guides (and their administrative policy settings) that can help individuals and organizations reduce the risk of unwanted interruptions, compromise, or exposure of sensitive data.

KISO recommends that administrators and users examine video conferencing tool user guides in their entirety; the links below are informational only and are not exhaustive. KISO is providing this general risk guidance and has not independently confirmed the veracity of each company's sites or claims. KISO does not certify, endorse, or recommend usage of one product over another product. Although administrators and users may improve video conference security by implementing capabilities noted below, cybersecurity events may still occur even if vendors and users take every possible precaution. KISO does not guarantee the security of these products; users are encouraged to verify, to every extent feasible, the security of vendor-provided products and to implement desired security controls.

<<SEE SECURITY SETTINGS TABLE ON NEXT PAGE>>

Security Settings Table

Product	Control Access	Connect Securely	File and Screen Sharing and Recording	Update Versions
Adobe Connect	Managing group policy			
	• Manage a meeting • Invite attendees and grant or deny access • Modify participant list • Remove individuals from a group	• Security overview • Secure connections	• Screen sharing controls • Sharing content • Recording and playback	• Application updates
Cisco WebEx	Managing group policy			
	• User management • Password settings	• Encryption	• Policy settings for screen, video, and file sharing	• Manual updates
GoToMeeting	Group Administration			
	• Password protect your meetings • Invite others • Manage attendees • Lock your meeting • One-time meetings	• Encryption	• Share your camera • Manage attendees • Share your screen • Keyboard and Mouse control • Record a session • Manage and share session recordings	• Automatic updates
GoToWebinar	• Password protect your webinar • Remove individual from webinar • Manage attendees	• Encryption and security features	• Screen sharing	• Automatic updates

Microsoft Teams	Managing policies in Teams			
	• Identification and authentication • Managing meeting policies • Assigning policies for users • Managing meeting settings • Control meeting participation • Control automatic meeting entry	• Communication and encryption	• Desktop sharing • Content sharing	• Teams updates
Slack	Slack workspace administration			
	• Manage members • Manage permissions	• Encryption	• Block download to unmanaged devices • Guest invitation • Screen sharing	• Download latest version
Zoom	Managing group policy in Zoom			
	• Assigning roles • Enable waiting rooms • Enable passwords • Identify guest participants • Enable two-factor authentication	• Encryption • Security settings • Audio watermark	• Limiting file types • Managing meeting participants (including screen sharing)	• Updates for Windows • Updates for MacOS • Updates for Android • Updates for iOS