Video Conferencing Standard

Introduction

State agencies rely on video conferencing and other collaboration solutions for employees to stay connected while teleworking. OMES is committed to balancing the cybersecurity requirements and risk exposure against remote access product benefits such as convenience, usability and stability.

Purpose

This document establishes the video conferencing standard for the State of Oklahoma, as well as requirements for using such services.

Standard

The State of Oklahoma standard for video conferencing is Microsoft Teams. Microsoft Teams has capacity and functionality that meets the needs of open meetings for most agencies. Zoom for Government is acceptable as it is Federal Risk and Authorization Program (FedRAMP) approved and meets the state's security requirements for voice, video and chat features.

Employees should exercise due diligence and caution in telework efforts. The following requirements can help mitigate teleconference threats.

- Users should connect securely by:
    - Change default password to strong, complex passwords for the router and Wi-Fi network.
    - Choose a generic name for home Wi-Fi network to help mask who the network belongs to, or its equipment manufacturer.
    - Ensure 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 the state for business use.
    - Enable security and encryption settings on video conferencing tools; these features are not always enabled by default.
- Host should control access by:
    - Require an access code or password to enter the event. **Do not** repeat codes or passwords.
    - Manage policies to ensure only members from the organization or desired group can attend. Be cautious of widely disseminating invitations.
    - Enable the waiting room feature to see and vet attendees attempting to access the event before the host grants access.
    - Lock the event once all intended attendees have joined.
    - Ensure the host 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) invitation links are disseminated.
- Host should manage file and screen sharing and recordings by:
    - 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 the meeting owner knows how to access and secure the recording. Change default file names when saving recordings. Consult with your organizational or in-house counsel regarding laws applicable to recording video conferences.
    - Consider sensitivity of data before exposing it via screen share or uploading it during video conferences. Do not discuss information that would not be discussed over regular telephone lines.
- All users should update to the latest versions of applications.
    - 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 the organization.

Compliance

This standard shall take effect upon publication and is made pursuant to Title 62 O.S. §§ 34.11.1 and 34.12 and Title 62 O.S. § 35.8. OMES IS may amend and publish the amended standards policies and standards at any time. Compliance is expected with all published policies and standards, and any published amendments thereof. Employees found in violation of this standard may be subject to disciplinary action, up to and including termination.

Rationale

To coordinate and require central approval of state agency information technology purchases and projects to enable the chief information officer to assess the needs and capabilities of state agencies as well as streamline and consolidate systems to ensure that the state delivers essential public services to its citizens in the most efficient manner at the lowest possible cost to taxpayers.

References

- Microsoft training for Teams.
- Zoom Learning Center.
- CISA Guidance for Secure Video Conferencing.

Revision history

This standard is subject to periodic review to ensure relevancy.

Effective date: 01/31/2022	**Review cycle:** Annual
Last revised: 01/31/2022	**Last reviewed:** 08/30/2023
Approved by: Joe McIntosh, Chief Information Officer	