Collaborative Computing Devices and Applications Standard

Introduction

The State of Oklahoma has a responsibility to protect state networks and the data/applications that flow across them. The Office of Management and Enterprise Services carefully reviews technology and makes recommendations on its use on state devices. In instances where the technology may pose a risk to state networks and data, the application or technology may be limited or prohibited. Collaborating computing devices pose potential security risks to State of Oklahoma users and data and must be appropriately managed to mitigate these risks.

Purpose

This standard applies to all collaborative computing technologies and establishes requirements for the authorization, configuration and use of collaborative computing devices and applications to prevent unauthorized access, reduce unintended exposure and ensure user awareness when collaborative capabilities are active.

Definitions

Collaborative computing device – a device that typically includes networking capabilities, cameras and microphones, enabling multiple users to work together on projects and tasks simultaneously.

Standard

Remote activation of collaborative computing devices and applications is prohibited by default. Collaborative computing devices and applications must be authorized in writing by the OMES chief information officer (CIO) or the CIO's designated representative. Each authorization shall explicitly identify:

- The approved collaborative computing mechanisms.
- The authorized purpose for use.
- The specific information system(s) or environment(s) on which the mechanisms may be used.

Collaborative computing devices and applications must provide a clear, explicit and continuous indication to users physically present at the device whenever collaborative capabilities are active.

Indications shall be sufficiently visible or audible to ensure users are aware of:

- Activation of microphones, cameras or recording functions.
- Active screen sharing or remote collaboration sessions.

Collaborative computing capabilities shall be configured to:

- Prevent unauthorized or unintended activation.
- Limit functionality to the minimum required to support the authorized process.
- Reduce the risk of inadvertent disclosure of information or monitoring of users.

All collaborative computing devices shall provide a clear, continuous visual indication when the device is in active use and shall display an explicit, real-time list of all participants connected to any meeting or session, regardless of the type of information being shared. This requirement

supports compliance with applicable regulatory frameworks, including but not limited to CJIS, IRS Pub. 1075, TSSR and ARC-AMPE.

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 ensure efficient, secure, and cost-effective delivery of essential public services, all state agency IT purchases and projects must receive central approval. This allows the Chief Information Officer to evaluate agency needs and capabilities, strengthen data protection and security, and streamline and consolidate systems to reduce costs for taxpayers.

References

- NIST SP-800-53, Rev 5, SC-15.

Revision history

This standard is subject to periodic review to ensure relevancy.

Effective date: 06/12/2026	**Review cycle:** Annual
Last revised: 06/12/2026	**Last reviewed:** 06/12/2026
Approved by: Dan Cronin, Chief Information Officer	