Azure Virtual Desktop Standard

Introduction
Azure Virtual Desktop is the cloud-based desktop and app virtualization service used by the State of Oklahoma to create a secure, resilient and reliable user desktop environment. AVD allows OMES IS to deploy virtual machines, specifically configured and securely instanced in the Azure cloud. Maintaining data integrity in this environment requires adherence to best practice security precautions.

Purpose
This document establishes security guidelines necessary to support the typical AVD environment.

Definitions
AVD – Azure Virtual Desktop; a scalable and flexible desktop virtualization environment.
RDP – Remote Desktop Protocol; a proprietary protocol developed by Microsoft, enabling users to connect to and control another Windows computer from a remote location.
AVD golden image – A single, base configuration for operating systems, applications and security tools upon which other packaged software may be installed via the state's client management system.

Standard
AVD environment requires specific controls and guidelines:

- Cyber Command is the system administrator. Administrative access is not provided to AVD session hosts, as it interferes with other devices within the same host.
- AVD projects require involvement from all the major stakeholders:
    - Project managers.
    - Technical architects.
    - Compliance officers.
    - Application managers.
    - Infrastructure engineers.
        - Cloud.
        - Network.
        - Server.
- Software requests must be routed through the user's direct manager for approval and installation on the AVD golden image. If the requested software is not on the OMES-approved software list, it must be approved before installation.
- Data storage:
    - All user data should be stored in OneDrive or a storage location separate from AVD. The AVD user profiles are not backed up and cannot be restored if corrupted.
    - User data stored on the local C: drive in AVD session hosts is not backed up or recoverable.
- AVD hosts will be restarted or reprovisioned as needed.
- The following RDP properties are enforced on AVD session hosts:
    - Allowed for redirection from the user's local host:
        - Microphone.
        - Speaker.

        - Cameras.
    - Disabled for redirection from the user's local host:
        - All local drives.
        - Clipboard.
    - Multi-monitor.
    - RDP-efficient multimedia streaming.
    - Auto-reconnect.
    - Automatic AVD session termination:
        - Screen lock after 15 minutes.
        - Disconnect idle sessions after 30 minutes.
        - Log off disconnected sessions after two (2) hours.
- CrowdStrike, NXLog agent, and Delinea PAM are installed on every AVD session host.

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
- Data Security Standard.

Revision history
This standard is subject to periodic review to ensure relevancy.

Effective date: 12/16/2025	**Review cycle:** Annual
Last revised: 12/16/2025	**Last reviewed:** 12/16/2025
Approved by: Dan Cronin, Chief Information Officer	