

Desktop Shortcut Icon Standard

Introduction

State employees and agencies have a need for the ability to locate core applications in an easy, seamless process. OMES is committed to solving customer needs by creating desktop and/or start menu shortcuts that link directly to core applications. This relieves users of time and frustration searching for core applications.

Purpose

To provide quick access to core applications while keeping the desktop environment clean.

Definitions

Desktop icon – a small, actionable graphical symbol on a computer's screen that represents programs, files, folders, or system utilities.

Core application – a fundamental, business-critical software program essential for an organization's daily operations.

Intune policy – Microsoft Intune policies are cloud-based rules and configurations deployed to devices and users to manage security, settings, and compliance.

Start menu – the primary user interface component in Microsoft Windows, located on the taskbar, acting as the central launching point for applications, files and system settings.

Standard

Desktop and start menu icon creation and deployment.

- Desktop and start menu shortcut icons must use consistent naming conventions. The application name must be clearly stated on the icon image, and the application description must be included in the icon text.
 - Ensures users across all agencies can immediately identify shortcuts without confusion, reducing service desk calls, emails and onboarding time.
- Ensure desktop and start menu shortcut icons are high resolution for clarity. Standard icon resolutions vary by platform, with 24 X 24 or 48 X 48 pixels being common for UI elements.
 - Crisp, clear icons prevent visual ambiguity and reinforce that the shortcut links to an officially sanctioned, trusted application.
- Desktop and start menu shortcut icons will be deployed by automated Intune Policy. Deployment of approved icons must be requested via a ServiceNow ticket. Requests must be submitted by program managers, system owners or department supervisors who ensure the requested shortcut pertains to official business and complies with organizational and security guidelines.
 - Intune Policy deployment guarantees that all in-scope machines receive the correct shortcut simultaneously, eliminates user error and creates a repeatable, auditable process that aligns with OMES's IT governance model.
- Review, update, remove unused or broken desktop and start menu shortcut icons yearly. Icons will be reviewed and/or updated by the application owner. Icons will be removed when an application is uninstalled or no longer required by agency policy.

- Stale shortcut icons clutter the desktop environment, erode user trust when they fail to launch and can point to decommissioned or vulnerable systems.

Approvals.

- Only approved, agency-standard applications should have default desktop shortcuts. OMES CIO written approval is required and should be requested and received via email. If approval is received, the approval email should be attached to a ServiceNow service request for a new icon deployment.
- Agencies shall not remove approved agency-standard application icons from the desktop and/or start menu without OMES CIO written approval. CIO approval shall be requested and received via email. If approval is received, the approval email should be attached to a ServiceNow service request for icon removal.

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.

Revision history

This standard is subject to periodic review to ensure relevancy.

| | |
|-----------------------------------------------------------|----------------------------------|
| Effective date: MM/DD/YYYY | Review cycle: Annual |
| Last revised: 5/14/2026 | Last reviewed: 05/14/2026 |
| Approved by: Dan Cronin, Chief Information Officer | |