OKLAHOMA
Office of Management
& Enterprise Services

# Caching Standard

## Introduction

Caching in-web and embedded applications is a useful and necessary tool to eliminate latency and provide an optimized experience for our stakeholders and clients. However, caution must be used with certain caching methods when dealing with sensitive citizen data.

## Purpose

The purpose of this document is to provide a standard for caching within client-facing (both public and non-public) applications.

## Definitions

Caching – The act of saving dynamic data/content to something (generally a text file or into memory) so that the content can be quickly recalled to screen upon re-access during a user's session. Caching can also be taken a step further where after initial cache, the content is saved into memory or a text file until a time period has passed and anyone, not just the initial user, can access the cached content until it has expired.

Cache-busting – Removing the cached content and requiring it to be recreated upon next view with the latest version of the dynamic data.

Dirty cache – Cached content that has not yet been re-accessed, but when it is re-accessed will be removed due its time limit for retention having expired.

## Standard

Expected types of caching covered by this standard include:

- Static web content (text, images, html) that is hard-coded.
- Application content.
- User-session-specific dynamic content that is converted to static web content.

It is expected that application and web developers should attempt to cache their static content that is non-sensitive and not listed below under "Restricted caching". This is done in a variety of ways and should be part of the development team's strategy to provide the best possible experience to our users.

Restricted caching.

Dynamic content that relates to a user's account should never be cached for anyone else except that user. This includes form data, user profile data and information about that user that may be protected by law (HIPAA, PCI, etc.) Great care should be taken that no sensitive data of one user can ever be seen by another user of the application.

## 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.

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

| | |
|---|---|
| **Effective date:** 05/24/2022 | **Review cycle:** Annual |
| **Last revised:** 05/24/2022 | **Last reviewed:** 02/03/20235 |
| **Approved by:** Dan Cronin, Chief Information Officer | |