



Tagging Governance Standard

Introduction

This standard establishes the mandatory resource tagging framework across all IT infrastructure environments managed or utilized by Oklahoma state agencies. By establishing a unified metadata baseline across cloud, on-premises and enterprise systems, this document ensures consistent asset visibility, interoperability and automated governance throughout the complete lifecycle of state IT assets.

Purpose

The purpose of this standard is to implement a structured resource tagging methodology that supports financial transparency, operational efficiency, regulatory compliance and automated asset management across state IT environments. Specifically, standardized metadata tagging enables agency cost allocation and chargeback, operational telemetry and observability, security and regulatory compliance and automated lifecycle and patch management.

Definitions

Agency number – the official four-digit numeric code designated by the State of Oklahoma to identify individual state agencies, boards and commissions for administrative, accounting and financial tracking.

Application/workload – a logical grouping of software components, databases and infrastructure assets that work together to deliver a specific business capability or service.

Chargeback – an accounting methodology where the direct costs of cloud infrastructure and IT resources are measured and allocated back to the specific agency or division consuming those services.

Data classification – the systematic categorization of state-held data based on its sensitivity, business impact and applicable regulatory compliance baselines (e.g., public, confidential, CJIS, PHI, PII, IRS 1075).

Hybrid infrastructure – an enterprise IT computing framework that integrates on-premises physical or virtualized data centers with one or more public cloud provider environments (e.g., AWS, Azure, GCP).

Lifecycle management – the designated operational deployment stage of a resource within the software development lifecycle (e.g., development, test, staging, production).

Metadata – structured data attached to an asset that describes, explains or gives operational context to that asset.

Resource tag – a metadata construct consisting of an assigned key-value pair attached directly to an infrastructure resource to enable identification, searchability, automation and governance.

Note: Multi-cloud providers implement metadata under different terms. In Google Cloud Platform (GCP), the term “label” corresponds to resource-level metadata and cost allocation, while “resource manager tag” corresponds to hierarchical policy enforcement and access control.

Standard

Key tagging principles:

- **Mandatory vs. optional tags:** Required tags must be applied at the time of resource creation. Optional tags may be applied to provide additional context where necessary.
- **Standardized case sensitivity:** Tag keys and values are strictly case-sensitive. Unless explicitly stated otherwise, all tag keys and standard values must follow kebab-case using only lowercase letters, numbers and hyphens to maintain compatibility across AWS, Azure and GCP character policies.
- **Inheritance:** Resources provisioned within structured containers must inherit mandatory tags applied at the parent container level unless overridden by asset-specific values. For cloud platforms that do not natively propagate metadata labels to child assets (e.g., GCP labels), automated provisioning pipelines must explicitly apply parent-level mandatory key-value pairs to child resources upon deployment.
- **Enforcement:** Compliance with these rules is enforced via automated policy engines. Non-compliant deployments will be restricted or flagged for immediate remediation.

Global tagging formatting rules: All tags must strictly adhere to the required syntax rules. Resources with malformed tags will be flagged for automated remediation or blocked at provisioning.

Mandatory required tags: Seven tags are mandatory on every server, virtual machine, database and cloud infrastructure resource and are strictly enforced. Automated provisioning gates will block the deployment of any resource lacking any of these seven tags. The required seven tags are platform, OS, tier, customer, env, service and team.

Recommended and contextual tags: Operational tags are strongly recommended for operational ownership, architectural mapping and security auditing. Specific regulated workloads may enforce them as conditional mandates.

Requirements:

- **Mandatory applicability:** All Oklahoma state agencies, organizational divisions and authorized third-party vendors must strictly comply with this standard when provisioning, configuring or modifying IT assets across state hybrid infrastructure and cloud environments.
- **Preventative enforcement:** Cloud environment guardrails and CI/CD deployment pipelines must enforce preventative checks that deny the provisioning of any compute, database or storage resource lacking any of the core seven mandatory tags.
- **Detective enforcement:** Automated compliance scanners evaluate all active assets against approved value dictionaries daily. Non-compliant casing, illegal characters or missing keys trigger automated incident tickets for remediation.
- **Tag inheritance:** Where cloud platform capabilities allow, resources should inherit default mandatory tags from parent containers. Agency resource owners remain ultimately responsible for verifying that all child assets carry valid tags.
- **Unassigned asset remediation:** Active resources carrying invalid or missing customer agency values are reassigned to an unallocated tracking account and escalated to enterprise leadership for mandatory attribution and remediation.

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: 10/08/2026	Review cycle: Annual
Last revised: 10/08/2026	Last reviewed: 10/08/2026
Approved by: Dan Cronin, Chief Information Officer	