OKLAHOMA
Office of Management
& Enterprise Services

# State Data Platform – Classification Standard

## Introduction

In order to manage who should have access to data and how it should be maintained over time, it needs to be appropriately classified by sensitivity and importance.

## Purpose

This standard provides a framework for data owners on the state data platform to appropriately classify data. It also ensures that all data stored on the platform is classified.

## Definitions

Glossary of Data-Related Terms (Oklahoma.gov).

NIST – National Institute of Standards and Technology.

Data classification – The process of organizing data by relevant categories so that it may be used and protected more efficiently.

HIPAA – Health Information Portability and Accountability Act.

FERPA – Family Educational Rights and Privacy Act.

DASH – (dash.ok.gov) A state-established data sharing application built on GCP with hub and spoke model. This application allows for secure inter/intra agency data sharing. DASH establishes key roles and responsibilities for data owner, data consumer and platform administrator.

Tag or label – Metadata added to files indicating the classification results.

DLP – Cloud data loss prevention.

Least privilege principle – Every process, user or program must be able to access only the information and resources that are necessary for its legitimate purpose.

Zero trust architecture – Entities are never implicitly trusted, but explicitly verified or authenticated.

Context-based classification – Inspects and interprets files to identify sensitive information.

User-based classification – Manual selection of each document by a person.

## Standard

All production data placed on the SDP is properly identified in accordance with OMES standards for classification.

- This includes but is not limited to:
  - Risk classification (DASH sensitivity classification: high, moderate, low) per NIST (NIST SP 800-60).

    - Identification of any federal or state privacy/confidentiality laws, administrative rules or business regulations (HIPAA, FERPA, 42CFR, IRS-1075) (DASH information type: HIPAA, FERPA).
- In DASH.
    - Identification of the classification tags is required information from the data owner (SME) during the data registration process (see DASH introduction). For all other data added to the SDP, classification tags are added at the data level.
- Data on SDP shall be classified in accordance with OMES data security classification standards.
- Audit for compliance.
    - Data on the SDP without proper data tags shall be identified and regular notification is sent to the data owner/agency project owner. An audit is performed quarterly and actions to remove/restrict shall be approved by the director of data driven services.
- Failure to follow the standard.
    - Production data not properly tagged via OMES classification standards is subject to removal and/or suspension of the data owner's access and privileges on the platform.

## 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

- ISO 27001.
- PCI-DSS.
- GDPR.
- National Institute of Standards and Technology (NIST), Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1, April 2018.
- NIST Federal Information Processing Standard (FIPS) 199, Standards for Security Categorization of Federal Information and Information Systems, February 2004.
- NISTS Internal Report (IR) 8112, Attribute Metadata: A Proposed Schema for Evaluating Federated Attributes, January 2018.
- NIST Privacy Framework: A Tool for Improving Privacy Through Enterprise Risk Management, Version 1.0, January 2020.
- NIST Special Publication (SP) 800-53 Rev. 5, Security and Privacy Controls for Information Systems and Organizations, September 2020.
- NIST SP 800-60 Vol. 1 Rev. 1, Guide for Mapping Types of Information and Information Systems to Security Categories, August 2008. Project Description: Data Classification Practices 9.
- NIST SP 800-171 Rev. 2, Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations, February 2020.

- NIST SP 800-207, Zero Trust Architecture, August 2020.

## Revision history

This standard is subject to periodic review to ensure relevancy.

| | |
|---|---|
| **Effective date:** 05/12/2022 | **Review cycle:** Annual |
| **Last revised:** 05/12/2022 | **Last reviewed:** 07/28/2023 |
| **Approved by:** Joe McIntosh, Chief Information Officer | |