OKLAHOMA
Office of Management
& Enterprise Services

Data Classification Security Standard

Introduction
The State of Oklahoma requires state-owned data to be classified and labeled based on the potential adverse impact due to loss of data confidentiality, integrity and availability. Classification and labeling are required to identify appropriate data protection measures.

Purpose
This document defines the requirements and guidelines for classifying state owned data.

Definitions
Availability – Ensuring timely and reliable access to and use of information.

Confidentiality – Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information.

Data classification – Organizing and identifying data by relevant categories so it may be used and protected more efficiently.

Integrity – Guarding against improper information modification or destruction and includes ensuring information non-repudiation and authenticity.

Provisional recommendations – A recommendation for impact determination based on information type. Provisional recommendations are subject to review and modification by agency stakeholders.

Standard
The State of Oklahoma's data are essential resources that must be protected from unauthorized use, access, disclosure, modification, loss or deletion. The appropriate level of physical, technical and administrative safeguards necessary to provide protection is relative to the potential impact in the event of loss of data confidentiality, integrity and availability.

Each Oklahoma agency shall classify its data and add metadata tags (labels) in accordance with this standard to ensure appropriate protections and consistence throughout the data life cycle. Data owners at the agency level are responsible for ensuring proper classification of data sets.

To ensure standardization across agencies, data sets shall be classified using high, moderate and low indicators based on potential impact in the event of a loss of confidentiality, integrity and availability. Agencies shall use the classification guidance detailed in the most current revisions of NIST 800-53R, NIST FIPS 199, and NIST 800-60 Volumes I and II.

At a minimum, data classification shall address the items listed below.

- Data type.
- Confidentiality impact.
- Integrity impact.
- Availability impact.
- Disaster Recover (DR) priority.
- Retention requirement – optional but should be included.

Data type

Data classification labels shall be used in each system, application and database having this functionality, and ServiceNow shall be used whenever possible to maximize centralization.

To classify data, the data type must first be identified. Identifying the data type provides information about the value, legal requirements, sensitivity and criticality of the data, which inform impact determinations.

All production level data sets must identify data type/what statutes or regulations apply (e.g., HIPAA, FERPA, IRS Pub.1075, GDPR, PCI requirements). A non-exhaustive list of common data types is included as Attachment 1, and agencies should consult NIST guidance, when classifying data.

Impact levels

Impact Level	**Definitions / Example**
Low	The loss of confidentiality, integrity, or availability could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals. Explanation: A limited adverse effect means that, for example, the loss of confidentiality, integrity, or availability might: (i) cause a degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of the functions is noticeably reduced; (ii) result in minor damage to organizational assets; (iii) result in minor financial loss; or (iv) result in minor harm to individuals. *Footnote: Adverse effects on individuals may include, but are not limited to, loss of the privacy to which individuals are entitled under law.
Moderate	The loss of confidentiality, integrity, or availability could be expected to have a serious adverse effect on organizational operations, organizational assets or individuals. Explanation: A serious adverse effect means that, for example, the loss of confidentiality, integrity or availability might: (i) cause a significant degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of the functions is significantly reduced; (ii) result in significant damage to organizational assets; (iii) result in significant financial loss; or (iv) result in significant harm to individuals that does not involve loss of life or serious life threatening.
High	The loss of confidentiality, integrity or availability could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets or individuals. Explanation: A severe catastrophic adverse effect means that, for example, the loss of confidentiality, integrity or availability might: (i) cause a severe degradation in or loss of mission capability to an extent and duration that the organization is not able to perform one or more of its primary functions; (ii) result in major damage to organizational assets; (iii) result in major financial loss; or (iv) result in severe or catastrophic harm to individuals involving loss of life or serious life-threatening injuries.

Disaster recovery

Additionally, a disaster recovery tier must be identified for each application as indicated below.

Tier	Definition
Tier 1: Mission Critical	Life safety and extreme business impact. Fundamental, essential business or technology functions or services required for the daily operation of the agency in order to complete their agency mission in part or while. In a disaster recovery mode, these are the first services restored. Failure of these services could result in life or safety issues or loss of revenue, or fines imposed on the agency by outside bodies.
Tier 2: High Priority	Severe business impact. Functions and services that are required for the agency to complete its mission (in part or in whole) but do not result in any life or safety issues. Interruption of these services can cause a hardship to staff and/or the public and prevent the agency from fully serving its business customer base.
Tier 3: Normal Priority	Medium to high business impact. Functions or services that support the agency mission but do not pose an immediate risk to the agency being able to serve its business customer base. Failure of this function or service may cause an inconvenience to staff but does not post any risk to life or safety.
Tier 4: Low Priority	Not critical but impacting. Functions or services that provide supplemental or auxiliary support to the technical or business functions of the agency. These functions and services do not contribute directly to the agency completing its missions but to provide additional detail, information, data or context to mission essential functions or services.

Retention requirements

Although not required for classification of information, documenting records retention/destruction requirements is key to ensuring proper maintenance of the records retention lifecycle.

With certain statutory exceptions, all state agencies, boards and commissions are required to establish and maintain ongoing programs for the efficient and economical management of records and have their programs approved by the Archives and Records Commission (67 O.S. Sec 206, 305).

Records disposition schedules are reviewed and approved by the Archives and Records Commission as provided in Chapter 10A of Title 67 of the Oklahoma Statutes and in the rules for the Commission as set out in Title 60 of the Oklahoma Administrative Code.

The following is an example of data classification.

- Agency A provides health care delivery services to beneficiaries. A data owner at agency A is classifying a data set that contains information about the agency's health care delivery services.
- The data owner must first determine what type of information is contained in the data. They review that data and determine that it contains PHI and is subject to HIPAA requirements.
- The data owner consults NIST SP 800-60 Volume II for guidance on how to classify this information and sees that the provisional recommendation for health care delivery service data is confidentiality of low, integrity of high) and availability of low). However, because the data set is subject to HIPAA, the data owner determines that the confidentiality impact determination should be raised to moderate.

- The data owner tags the data set in the appropriate system as confidentiality of moderate, integrity of high and availability of low. The data owner must also tag the data set with the information the data type/applicable regulation (HIPAA) and must designate a disaster recovery tier for the data or application, as applicable. The data owner consults the disaster recovery tier table in this standard and determines that failure of the application housing the data, would result in a severe business impact, so the data owner designates disaster recovery tier 2 for the application. The data owner should also record the applicable record retention citation.

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

- Oklahoma Libraries Records Management.
- Oklahoma Libraries Records Scheduling.
- Consolidated General Records Disposition Schedule.
- NIST Federal Information Processing (FIPS) 199, Standards for Security Categorization of Federal Information and Information Systems.
- NIST SP 800-60 Vol 1 Rev 1, Guide for Mapping Types of Information and Information Systems to Security Categories.
- NIST SP 800-60 Vol. 2 Rev. 1, Appendices to Guide for Mapping Types of Information and Information Systems to Security Categories.
- NIST Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1.
- NIST Internal Report 8112, Attribute Metadata: A proposed Schema for Evaluating Federated Attributes.
- NIST Privacy Framework: A tool for Improving Privacy Through Enterprise Risk Management, Version 1.0.
- NIST SP 800-53 Rev. 5, Security and Privacy Controls for Information Systems and Organizations.
- NIST SP 800-154, Guide to Data-Centric System Threat Modeling.
- NIST SP 800-171 Rev. 2, Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations.
- NIST SP 800-207, Zero Trust Architecture.

Revision history

This standard is subject to periodic review to ensure relevancy.

Effective date: 04/13/2022	**Review cycle:** Annual
Last revised: 12/12/2022	**Last reviewed:** 08/02/2023
Approved by: Joe McIntosh, Chief Information Officer	

Attachment 1

The following table lists commonly encountered data types along with authorities that protect them, if applicable. This is not an exhaustive list of every data type an agency may encounter or every legal authority that applies. Where the Data Type column notation references a statute or regulation (e.g., DPPA) this is meant as quick reference for information that is subject to that regulation. For example, while Driver's Privacy Protection Act (DPPA) is not itself a data type, the agency data owner is expected to tag information subject to the DPPA with DPPA as an information type.

Additionally, some data may be protected by multiple statutes or regulations.

Data Type	**Description/Authority**	**Citation**
Open – public record	Oklahoma Open Records Act	51 O.S. § 24A.1 et seq.
Adult criminal protected information	Adult criminal records protected by state or federal statutes or regulations	*
Public assistance records	Applicant/beneficiary/recipient of public assistance programs	56 O.S. § 183 and 45 CFR § 205.50
APS case information	Adult Protective Services (APS)	43A O.S. §§ 10-110 and 10-110.1
CJIS	Criminal Justice Information Services Information	28 U.S.C. §534 and 28 CFR Part 20
Child welfare/juvenile deprived	Oklahoma Children's Code	10A O.S. §§ 1-2-108 and 1-6-102
Adoption information	Oklahoma Adoption Code	10 O.S. 7505-1.1; § 10 O.S. 7510-1.5
DPPA	Driver's Privacy Protection Act (DPPA)	18 USC §2721, et seq.
FERPA	Family Educational Rights and Privacy Act	20 U.S.C. § 1232g; 34 CFR Part 99
GDPR	General Data Protection Regulation	(EU) 2016/679
Income Information		*
FTI	Federal Tax Information	IRS 1075 Publication Rev 11-2021 / Internal Revenue Code (IRC) § 6103(p)(4)
Juvenile/youthful offender	Youthful Offender Act; also, OSBI records per 74 O.S. §150.9(C)	10A O.S. §§ 2-5-204-205 and 2-6-102; 74 O.S. § 150.9(C)
PCI	Payment Card Industry Data Security Standards	PCI DSS v4.0
PHI - HIPAA	The Health Insurance Portability and Accountability Act	Pub. L. No. 104-191
SSA Data	SSA provided information (PII)	Privacy Act, 5 U.S.C. 552a, section 1106 of the Social Security ACT and SSA's disclosure regulations.

PHI – substance use (federally assisted programs)	Confidentiality of Substance Use Disorder Patient Records	42 C.F.R. Part 2
PHI – mental health/drug or alcohol abuse	Confidentiality of Alcohol and Drug Abuse Patient Records	43A O.S. § 1-109
PII - other	Personally identifiable information	*
PII - Public Health Investigations	Public Health Code	63 O.S. § 1-502.2
PHI - Oklahoma Health Care Information System	Oklahoma Health Care Information System Act	63 O.S. § 1-120

* The agency data owner should determine what legal authorities apply, if any, and provide the applicable citation.