



State of Indiana Standard: Data Governance

Version: 1.0 (5/2026)

Contents

1. Purpose	2
2. Applicability.....	2
3. Revision History.....	2
4. Authority	2
5. Ownership.....	2
6. Definitions.....	3
7. Background	4
8. Standard.....	4
8.1. Federated Responsibilities	4
8.2. Statewide Coordination	5
8.2.1 Data Governance Council.....	5
8.2.2 Capability Assessments	5
8.3 Core Governance Roles.....	5
8.3.1 Statewide Roles.....	5
8.3.2 Designated Agency-level Roles.....	6
8.3.3 Coordination Between Roles.....	7
8.3.4 Functional Roles	7
8.4 Minimum Agency Practices.....	8
8.4.1 Roles and Accountability.....	8
8.4.2 Inventories and Classification	8
8.4.3 Privacy Impact Assessments	8
8.4.4 Data Sharing	8
9. References.....	10



State of Indiana Standard: Data Governance

Version: 1.0 (5/2026)

1. Purpose

The purpose of this Standard is to establish a statewide data governance baseline for State of Indiana agencies. This Standard is intended to support the efficient and appropriate use of data in service of Hoosiers. This Standard brings together existing Office of the Chief Data Officer (OCDO) policies, standards, and guidance related to data governance. It sets out a common governance model, defines key roles, and identifies minimum agency practices so that data governance requirements are applied consistently across State government.

2. Applicability

This Standard shall apply to all Data Governance as defined herein.

3. Revision History

Version	Date	Name	Revision Description	Supersedes
1.0	5/2026	C. Weiland J. Stark	Initial version.	n/a

4. Authority

This Standard is promulgated by the Office of the Chief Data Officer pursuant to IC 4-3-26-10(3). The OCDO may further promulgate component policies and/or subordinate standards, procedures, or guidance documents.

5. Ownership

Please direct questions and concerns to the following owner(s) of this Standard:

1. The State Chief Data Officer



State of Indiana Standard: Data Governance

Version: 1.0 (5/2026)

6. Definitions

1. “Data” means Government Information as set forth in IC 4-3-26-7
2. “Data Asset” means Data, a Data Collection, or related information resources that have business, operational, legal, or analytical value to the State or an agency
3. “Data Catalog” means a repository of metadata and related information used to identify, describe and support discovery and governance of Data and Data collections
4. “Data Classification” means the categorization of Data based on key attributes relevant to its handling including privacy risk, security risk, regulatory requirements, releasability, retention, and storage considerations
5. “Data Collection” means the categorization of Data based on key attributes relevant to its handling, including privacy risk, security risk, regulatory requirements, releasability, retention, and storage considerations.
6. “Data Governance” means the policies, procedures, and organizational structures that guide decision making and accountability.
7. “Data Management” means the planning, collection, use, maintenance, protection, sharing and improvement of Data throughout its lifecycle.
8. “Data Quality” means a measurement of qualitative and quantitative conditions that determine whether the data is fit-for-purpose in a business process or operation.
9. “Data Sharing” means the authorized exchange, disclosure, or provision of Data between agencies programs, systems, or approved third parties for a lawful purpose and in accordance with applicable law, policy, and agreement requirements.
10. “Federated Governance Model” means a governance approach in which common statewide policies, standards, and guidance are established centrally, while agencies retain responsibility for implementation and management of their data in accordance with those sitewide requirements
11. “Interoperability” means the ability of systems, applications, or data environments to exchange Data and use that Data effectively and consistently for authorized purposes.
12. “Inventory” means a maintained record of a system, data source, Data Collection, or Data Asset, and its relevant attributes, including, as applicable, ownership or stewardship, classification, retention, regulatory considerations, releasability, and storage information.
13. “Privacy Impact Assessment” means a methodological approach for assessing the privacy aspects of an information system that processes personal information.
14. “Sensitive Information” or “Sensitive Data” means Data requiring heightened protection due to legal, contractual, privacy, security, or operational considerations.



State of Indiana Standard: Data Governance

Version: 1.0 (5/2026)

7. Background

Through the daily operations of agencies, the State of Indiana collects, processes, and stores vast amounts of citizen and government data. Data, created and collected, from more avenues than ever before, is an asset when handled appropriately. With appropriate data governance, data empowers agencies to govern in the modern era by effectively delivering constituent services, informing policymakers to enable data driven policy outcomes, and driving overall improvements in operational efficiency. Ensuring that data is managed appropriately—of high quality, secure, and fit for purpose is central to the State’s mission.

8. Standard

The State of Indiana operates a federated approach to data governance. Under this model, the OCDO sets statewide standards, publishes policies and guidance, and provides consultative support to agencies through the Management Performance Hub’s (MPH) Data Governance team. Agencies govern the data they create, collect, process, and store, applying statewide standards to their specific operational context.

A federated approach balances unified data governance standards with operational flexibility. Agencies know their data the best and are better positioned to make day-to-day operational governance decisions. The OCDO ensures data interoperability, reduces duplicative efforts, and provides shared resources so that agencies are not building data governance frameworks from scratch. The result is a system where accountability stays close to the work, while common standards make it easier to share data and collaborate across agency boundaries.

8.1. Federated Responsibilities

Enterprise Level (OCDO): Sets statewide policies, standards, and guidance for data governance, data quality, and supporting disciplines. Maintains consistency across the State of Indiana executive branch by leading policy, standard, and guidance development and enterprise data tool selection. Provides support to agencies through capability assessments, training, templates, and consultative assistance.

Agency Level: Creates and implements a data governance program in day-to-day operations of the agency in accordance with enterprise standards. Designates required roles (Data Steward, Data



State of Indiana Standard: Data Governance

Version: 1.0 (5/2026)

Stakeholder, etc.). Establishes and maintains a holistic, agency wide data catalog that is interoperable with enterprise cataloging solutions. Applies statewide classification and sensitivity requirements. Ensures compliance with statewide policies within the agency's programs and operations.

Program Level: Program managers and Data Owners make purpose-driven decisions about how data is collected, used, and shared within their areas of responsibility. They apply statewide classification and privacy requirements to specific operational contexts and escalate governance questions to the agency Data Steward or Agency Privacy Officer (APO) as appropriate.

8.2. Statewide Coordination

The OCDO coordinates data governance efforts across the State through formal governance bodies and direct agency support.

8.2.1 Data Governance Council

The [Data Governance Council](#), chaired by the State Chief Data Officer, serves as the primary body for cross-agency coordination on data governance matters. The Council provides a forum for agencies to discuss common challenges, align practices, and advise on policy development from the agency perspective. See the Data Governance Council Charter for additional information on membership and operations.

8.2.2 Capability Assessments

The OCDO uses the Data Management Capability Assessment (DCAM) as the primary framework for assessing agency data management and governance maturity. Agencies may request DCAM-based assessments through the OCDO to identify strengths, gaps, and improvement opportunities.

8.3 Core Governance Roles

The federated governance model depends on clearly assigned responsibilities at the statewide, agency, and program levels. Statewide roles provide policy direction, coordination and support. Agency-level roles are responsible for implementing statewide expectations within agency operations. Program and functional roles apply governance practices to specific Data Assets, systems, Data Collections, and business processes.

8.3.1 Statewide Roles



State of Indiana Standard: Data Governance

Version: 1.0 (5/2026)

At the statewide level, two roles provide leadership and coordination for data governance across State government. These roles ensure consistent policy, enable cross-agency collaboration, and provide agencies with a central point of contact for governance matters.

State Chief Data Officer (State CDO): The Office of the Chief Data Officer (CDO) was established as part of [IC 4-3-26](#), along with the Indiana Management Performance Hub (MPH), on July 1, 2017. The CDO serves as the executive head of MPH and advises executive state agencies and political subdivisions regarding state best practices concerning the creation and maintenance of data. Additionally, the CDO coordinates data analytics and data master planning for the executive state agencies and provides leadership regarding state data analytics and transparency.

State Chief Privacy Officer (State CPO): Advises agencies on the application and enforcement of the Indiana Fair Information Practices Act, OCDO privacy policies, and general privacy best practices, serves as an advisor for interagency and public-private initiatives involving Personal Information, reviews and approves Data Sharing Agreements, and coordinates the network of Agency Privacy Officers.

These roles are supported by OCDO and MPH staff who provide technical assistance, facilitate capability assessments, develop and maintain statewide policies and guidance, and coordinate cross-agency governance activities.

8.3.2 Designated Agency-level Roles

At the agency level, data governance depends on clearly assigned responsibility for data and privacy. Each agency shall designate one Data Steward and an APO. In agencies with greater size, complexity, or data volume, an Agency Data Officer should also be designated to provide agency-wide leadership for data governance. Additional supporting roles, including Data Owner, Data Custodian, and Data Stakeholder, contribute to governance within their respective areas of responsibility.

The roles described below may be combined in smaller agencies where a single individual fulfills multiple functions. In larger agencies, multiple individuals may be designated to each role, aligned to programs, divisions, or data domains. Often, this position is already in existence and operation but is not formally defined and declared. Regardless of agency size, the functions described must be addressed and documented.

Agency-level roles operate within the federated model. Agency Privacy Officers coordinate with the State Chief Privacy Officer on privacy matters. Agency Data Officers and/or Data Stewards consult with OCDO on governance and data quality initiatives.

Agency Data Officer or Data Steward



State of Indiana Standard: Data Governance

Version: 1.0 (5/2026)

Agencies shall assign responsibility for day-to-day data governance. Each agency shall designate at least one Data Steward, as established in State of Indiana Policy: Information Quality. In smaller agencies, these responsibilities may be carried out without a separate Agency data officer designation. In larger agencies, an Agency data officer should provide agency-wide leadership for data governance, while one or more Data Stewards support implementation across programs, divisions, data domains, or major Data Collections.

For each key dataset, system, or published data visualization, one steward of record should be identified so that quality, documentation, and governance decisions have a clear point of accountability.

For detailed responsibilities related to data quality management, see [State of Indiana Policy: Information Quality, Section 7.1.](#)

Agency Privacy Officer

Agency Privacy Officers are the agency's lead for privacy risk and ensure the appropriate protection of personal and sensitive information. As established in State of Indiana Policy: Information Privacy, each agency shall designate an APO. The APO interprets statewide privacy expectations for the agency's programs and works with Data Stewards, Data Owners, and technical staff to ensure those expectations are met.

For detailed APO responsibilities, see [State of Indiana Policy: Information Privacy](#) and the [OCDO Standard: Agency Privacy Officer Job Description](#).

8.3.3 Coordination Between Roles

Agency Data Officers and/or Data Stewards, and APOs serve complementary functions. Agency Data Officers and Data Stewards focus on whether data is accurate, usable, and well-managed for operations, reporting, and analytics. APOs focus on whether data is collected, used, shared, and retained in ways that are lawful and aligned with statewide privacy expectations. Agencies shall involve these roles whenever decisions affect how data is used.

8.3.4 Functional Roles

Data Owner: Works with the Data Steward on governance and quality matter and with the APO on privacy risk. Makes decisions about access and use within the boundaries set by statewide Standard.

Data Custodian: The individual or function responsible for the technical environment in which data is stored, including security controls, backup, and system availability.



State of Indiana Standard: Data Governance

Version: 1.0 (5/2026)

Data Stakeholder: Any individual who uses or relies on data in their work and is responsible for following established guidelines and contributing to data quality.

8.4 Minimum Agency Practices

To comply with this Standard and related statewide policies, each agency shall, at minimum, implement the following practices. These requirements are established by the source policies referenced below; this section consolidates them for convenience.

8.4.1 Roles and Accountability

1. Designate an Agency Privacy Officer. (Information Privacy Policy, Sec 8.1)
2. Designate at least one Data Steward. (Information Quality Policy, Sec 7.1)
3. Identify and document Data Owners for key systems and data collections so that governance decisions have a clear owner. (Information Quality Policy, Sec. 7.1)

8.4.2 Inventories and Classification

1. Maintain an inventory of information systems and processes that collect, store, or process significant data assets, and update this inventory as systems are added, changed, or retired. (Information Privacy Policy, Sec. 8.2.3)
2. Establish and maintain an agency data catalog to document data assets, their owners, and classification.
3. Apply the statewide data classification scheme to systems and Data Collections in the inventory and handle data in accordance with the applicable classification and associated security, privacy, and handling requirements. (Information Privacy Policy, Sec. 8.2.2; OCDO Standard: Indiana Privacy Program Data Classifications)
4. Implement the [NIEM 6.0 data standard](#) , where applicable.

8.4.3 Privacy Impact Assessments

1. The APO shall ensure an annual review of the system and process inventory to determine where a PIA is required under statewide privacy policy. (Information Privacy Policy, Sec. 8.2.1)
2. The APO shall ensure that PIAs are completed for new or significantly changed systems that process personal Information, in accordance with the State of Indiana Policy: Information Privacy and the State of Indiana Standard: Privacy Impact Assessment Methodology. (Information Privacy Policy, Sec. 8.2.1)

8.4.4 Data Sharing



State of Indiana Standard: Data Governance

Version: 1.0 (5/2026)

1. When sharing personal information or other sensitive data outside the agency, the agency shall verify that sharing is permitted under applicable law. (Information Privacy Policy, Sec. 8.3.1)
2. The agency shall use a data sharing agreement approved by the State CPO, following the prescribed process, when required by state policy. (Information Privacy Policy, Sec. 8.3.1)



State of Indiana Standard: Data Governance

Version: 1.0 (5/2026)

9. References

1. State of Indiana Policy: *Information Privacy*, <https://www.in.gov/mph/cdo/files/State-of-Indiana-Information-Privacy-Policy.pdf>
2. State of Indiana Policy: *Artificial Intelligence*, <https://www.in.gov/mph/cdo/files/State-of-Indiana-Artificial-Intelligence-Policy.pdf>
3. State of Indiana Policy: *Fair Information Practices related to Agency Analytics Environments*, <https://www.in.gov/mph/cdo/files/20230522-FINAL-State-of-Indiana-Policy-Fair-Information-Practices-related-to-Agency-Analytics-Environments.pdf>
4. State of Indiana Policy: *Information Quality*, <https://www.in.gov/mph/cdo/files/State-of-Indiana-Information-Quality-Policy.pdf>
5. DCAM (Data Management Capability Assessment Model), EDM Council, <https://edmcouncil.org/frameworks/dcam/>
6. OCDO Standard: *Indiana Privacy Program Data Classifications*, <https://www.in.gov/mph/cdo/files/20230706-FINAL-OCDO-Standard-Privacy-Data-Classification.pdf>
7. State of Indiana Standard: *State Agency Artificial Intelligence Systems*, <https://www.in.gov/mph/cdo/files/State-of-Indiana-Artificial-Intelligence-Policy.pdf>
8. State of Indiana Standard: *Privacy Impact Assessment Methodology*, <https://www.in.gov/mph/cdo/files/State-of-Indiana-Standard-PIA-Methodology.pdf>
9. Data Governance Council Charter, <https://www.in.gov/mph/cdo/files/Data-Governance-Charter-Final.pdf>
10. OCDO Standard: *Agency Privacy Officer*, <https://www.in.gov/mph/cdo/files/20230715-FINAL-OCDO-Standard-Agency-Privacy-Officer.pdf>