ARIZONA DEPARTMENT OF ADMINISTRATION	STATEWIDE POLICY	State of Arizona

P4470 DATA GOVERNANCE DOCUMENTATION POLICY

DOCUMENT NUMBER:	P4470
EFFECTIVE DATE:	FEBRUARY 7, 2023
VERSION:	2.0

1. AUTHORITY

To effectuate the mission and purposes of the Arizona Department of Administration (the "Department"), the Department shall maintain a "coordinated statewide plan for information technology" implemented and maintained through policies, and "adopting statewide technical, coordination and security standards" as authorized by Arizona Revised Statute (A.R.S.) § 18-104 A.1.(a). The Department shall also "formulate policies, plans and programs to effectuate the government information technology purposes of the department" pursuant to A.R.S. § 18-104 A.13.

2. PURPOSE

2.1 The purpose of this policy is to establish statewide documentation practices in the following areas:

2.1.1 Data modeling – defining and documenting the structure, organization and interrelationships of data;

2.1.2 Data flow – defining and documenting relationships among and between the various data components in a program or system;

2.1.3 Metadata – data that describes data structure, classification, business concepts and technical attributes of data; and

2.1.4 Data Classification – defining and documenting the privacy and risk classification of data.

3. SCOPE AND APPLICABILITY

3.1 This policy applies to all employees and contractors within State Budget Units (BU) who work with data or repositories of data while executing business functions, activities or services for or on behalf of the BU or its customers.

3.2 This policy applies to all Covered Information Systems as defined in P4400 Data Governance Organization Policy and designated as such by the Data Governance Council of the BU.

3.3 Specific standards issued under this policy may extend applicability beyond Covered Information Systems.

3.4 Applicability of this policy to third parties is governed by contractual agreements entered into between the BU and the third party. For contracts in force as of the effective date, subject matter experts (SMEs) acting under direction of the Data Policy Council, shall review the applicability of this policy to third parties before seeking amendments. Prior to entering into new contracts, SMEs shall ascertain the applicability of this policy to third parties and include compliance requirements in the terms and conditions.

3.5 With respect to all other Information Systems in service as of the Effective Date, implementation of this policy is recommended but is not mandatory. If such systems are already compliant as of the Effective Date, procedures to keep them compliant for the remainder of their lifetime should be implemented or continued.

3.6 This policy shall be referenced in Business Requirements Documents, Requests for Information, Requests for Proposal, Statements of Work and other documents that specify the business and technical specifications of Information Systems being developed, maintained, or procured.

3.7 State BUs and third parties supplying information systems to other BUs or developing information systems on behalf of a BU shall be required to comply with this Policy including documentation to demonstrate compliance with all State policies and documented security controls.

3.8 This policy does not apply to file systems, file repositories, electronic documents, images or other files.

4. Roles And Responsibilities.

4.1 The Chief Executive Officer (Director) of the BU or his/her designee shall ensure the effective implementation of Information Technology Policies, Standards, and Procedures (PSPs) within the BU.

4.2 BU Supervisors shall ensure that employees and contractors are appropriately trained and educated on this Policy and shall monitor employee and contractor activities to ensure compliance.

4.3 Employees and contractors shall adhere to all state and BU policies, standards and procedures pertaining to the use of the State IT resources.

4.4 The Enterprise Data Management Officer, Data Policy Council, Data Management Committee, Data Owners, Data Custodians and Data Stewards shall be designated and shall carry out the duties assigned to them under P4400 – Data Governance Organization Policy and any other duties assigned to them under this Policy.

5. POLICY

5.1 BUs shall create, update and maintain throughout the life cycle of a Covered Information System a metadata repository for the Information System's data. The metadata repository should provide the following:

5.1.1 A business glossary, defining the BU's common business terms;

5.1.2 A data catalog, describing the physical, logical and business meaning of the data;

5.1.3 Data lineage, describing the data flow, origins of the data, where it's used and how it flows through the systems;

5.1.4 Data classification, as further described below.

5.2 Business requirements, budgets, project plans and related documents prepared for any project shall include the procedures and resource budget necessary for compliance with this policy. The absence of a project requirement to comply with this policy, or the failure to allocate time and resources to the underlying tasks shall not justify its omission from the project nor absolve the project stakeholders from compliance.

5.3 BUs shall provide appropriate tools, training and a document repository to facilitate compliance with this policy by employees and contracted third parties. These tools will be referred to as Data Management Tools.

5.4 The following Data Management Tool capabilities and process methodologies shall be utilized in compliance with this Policy:

5.4.1 Data flow diagrams and data modeling tools and methodologies should conform to a consistent methodology to be approved by the BU Data Management Office with recommendations from the Data Governance Council based on the needs of the BU. Users shall be trained to use the chosen methodology and budget shall be allocated for such training.

5.4.2 Metadata repositories should be selected and approved by the BU Data Management Office with recommendations from the Data Governance Council based on the needs of the BU.

5.4.3 If a given project or implementation wishes to make use of a methodology or tool that does not comply with these recommendations it may be substituted with another tool or methodology under the following conditions:

5.4.3.1 The reasons for choosing an alternate tool or methodology and the costs and risks of using an alternate tool or methodology shall be documented and evaluated;

5.4.3.2 Necessary and sufficient business processes and training shall be provided to mitigate the risks, minimize the costs and successfully implement the alternate technology or methodology in a sustainable manner; and

5.4.3.3 The alternate technology or methodology, business processes, training and implementation plans shall be reviewed and approved for use by the Chief Information Officer upon the recommendation of the Data Management Committee.

5.5 BUs shall classify their data and store the classification in the metadata repository.

5.5.1 Classification Definitions by Privacy – Data shall be classified according to its degree of sensitivity into the categories specified in Statewide Policy P8110 - Data Classification. This classification will be referred to as the Privacy Classification.

5.5.2 Classification Definitions by Risk – Risk levels shall be assigned based on the impact of a security breach or disclosure event based on P8120 Information Security Program.

5.5.3 Transitional provisions

5.5.3.1 Data that has not yet been subjected to a classification process, or for which the classification is unknown or missing, is deemed to be Confidential.

5.5.3.2 Data should be classified prior to fulfilling any public record request relating to the data specified in the request.

5.5.3.3 Data Owners or Data Domain Stewards shall submit a plan to the Director within 180 days of the effective date of this Policy whereby data will be explicitly classified by a specified date.

5.5.4 Additional Classifications – BUs requiring additional classifications may create and document those classifications and any related procedures and responsibilities at their discretion.

5.5.5 Data Owners shall ensure that procedures are established, responsibilities assigned, and training is provided for the following:

5.5.5.1 Data Owners shall delegate Stewardship, access and custody of data in accordance with P4400 - Data Governance Organizational Policy and P4450 - Data Governance Data Operations Policy;

5.5.5.2 At the time of designing, specifying, installing or implementing a Covered Information System, the Data Owner shall ensure that confidential data elements are identified and appropriate procedures and security controls are implemented to maintain and to manage access to them. Such procedures shall include ensuring that security personnel charged with managing access to such data or databases are informed of the sensitivity of any data stored by the application and of the procedures to obtain approvals to access it.

5.5.5.3 At the time of designing, specifying, installing or implementing a Covered Information System, the Data Owner shall ensure that points of access to or exposure of Confidential data elements, such as display screens, dialogs or reports are identified and appropriate procedures and security controls are implemented to manage access to them. Such procedures shall include ensuring that security personnel charged with managing access to such applications shall be informed of the sensitivity of such applications and the procedures to obtain approvals to access it;

5.5.5.4 At the time an Information System is decommissioned, archived, deleted, or removed from service, the presence of any Confidential data elements shall be identified and appropriate procedures implemented to ensure that the Confidential data remains under appropriate security controls as long as the data continues to exist;

5.5.5.5 At the time a document containing confidential elements is created, procedures and technical tools to support the procedures shall be used to classify the document and protect it accordingly;

5.5.5.6 The Data Management Committee shall be informed about the presence of Confidential Data in any Covered Information Systems in their purview and shall implement the necessary procedures to abide by any relevant statute, law or policy;

5.5.5.7 At the time custody of physical media containing Confidential data is changed, the new Custodian shall be apprised of the classification of data on that media and abide by any statute, law or policy;

5.5.5.8 Data must be classified prior to being stored in or moved to hosted services;

5.5.5.9 At the time physical media is taken out of service, all Confidential data on that media shall be erased using secure procedures that overwrite the media in accordance with NIST standards. A certificate shall be provided to the General Services Division or other entity taking custody of that media attesting to the secure destruction of Confidential data. (NIST 800-53 v4].

5.6 The BU shall ensure that projects and anticipated investments related to the implementation of this policy are included in the BU's annual IT Strategic Plan.

5.7 Implementation Guidance – BUs should plan to implement this policy for Covered Information Systems by the end of the 2025 Fiscal Year.

5.7.1 BUs that are unable to commence implementation of this policy by the 2025 Fiscal Year may apply for an extension of time by following the process outlined in Statewide Standard S4470 - Data Governance Documentation Extension.

5.7.2 A BU may designate an Information System as exempt from this requirement if it is expected to be rendered obsolete by a planned replacement of the system.

5.7.3 A BU is considered compliant with the *implementation* of this policy if the following are true:

5.7.3.1 The BU has acquired or designated a product, platform or other repository to house the metadata, and

5.7.3.2 The BU has documented processes and procedures to populate metadata in the repository, and evidence that they are being carried out, and

5.7.3.3 The repository has sufficient metadata in it to satisfy one or more business use cases for the repository.

6. Definitions And Abbreviations

Refer to the PSP Glossary of Terms located on the ADOA-ASET website.

7. REFERENCES

A.R.S. § 18-104

ASET P4400 - Data Governance Organization Policy

8. VERSION HISTORY

Date	Change	Revision	Signature
2/07/2023	Major revision	2.0	J.R. Sloan, State CIO
6/30/2019	Initial Release	1.0	Morgan Reed, State CIO and Deputy Director