ARIZONA DEPARTMENT OF ADMINISTRATION	**Statewide** **POLICY**	**State of Arizona**

P4470 DATA GOVERNANCE DOCUMENTATION POLICY

DOCUMENT NUMBER:	**P4470**
EFFECTIVE DATE:	**JUNE 30, 2019**
REVISION:	**1.0**

1. AUTHORITY

To effectuate the mission and purposes of the Arizona Department of Administration (ADOA), ADOA shall establish a coordinated plan and program for information technology (IT) implemented and maintained through policies, standards and procedures as authorized by Arizona Revised Statutes (A.R.S.) § 18-104.

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. EXCEPTIONS

4.1 Policies, Standards and Procedures may be expanded or exceptions may be taken by following the Statewide Policy Exception Procedure.

5. ROLES AND RESPONSIBILITIES

5.1 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.

5.2 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.

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

5.4 The 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.

6. POLICY

6.1 BUs shall complete, update and maintain throughout the life cycle of a Covered Information System at a minimum the Physical Data Model and Physical Data Flow Diagram and the metadata repository for the Information System's data. BUs may include the Conceptual Data Model, Logical Data Model, Conceptual Data Flow Diagram and Logical Data Flow Diagrams.

6.2 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.

6.3 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.

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

6.4.1 Data flow diagrams and data modeling tools and methodologies should conform to a consistent methodology to be recommended and adopted by the Data Management Committee based on the needs of the BU. Users shall be trained to use the chosen methodology and budget shall be allocated for such training.

6.4.2 Metadata repositories should conform to ISO 11179 or to another standard approved by the Chief Information Officer upon the recommendation of the Data Management Committee based on the needs of the BU.

6.4.3 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:

a) 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;

b) 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

c) 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.

6.5 Data Classification

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

6.5.2 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.

6.5.3 Transitional provisions

a) 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.

b) Data shall be classified prior to fulfilling any public record request relating to the data specified in the request.

c) Data Owners 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.

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

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

a) 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;

b) 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.

c) 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;

d) 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;

e) 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;

f) 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;

g) 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;

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

i) 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]

7. DEFINITIONS AND ABBREVIATIONS

7.1 Data Model - Definition

7.1.1 A data model is a representation of the structure, organization and interrelationships of data. A data model can be conceptual, logical or physical.

a) A conceptual model articulates the data concepts and their relationships. This describes the semantics of an organization and represents a series of assertions about its nature.

b) A logical model defines data structures such as relational tables and columns, object-oriented classes, or XML tags.

c) A physical data model represents the physical structure of the data or database.

7.2 Data Flow Diagram - Definition

7.2.1 A Data Flow Diagram (DFD) is a graphical depiction of the relationships among and between the various components and processes in a program or system. They depict how input data is transformed to output results through a sequence of functional transformations and consist of four major components - entities, processes, data stores, and data flows. A DFD can be conceptual, logical or physical.

a) A conceptual DFD focuses on transformation of concept values.

b) A logical DFD focuses on the business processes surrounding the data flow.

c) A physical DFD focuses on the implementation of the data flow and includes manual process details and data structures.

7.3 Metadata – Definition

7.3.1 Metadata is data that describes attributes of the underlying data. These attributes include classification, physical structure, logical definition and business concepts represented in the data.

7.3.2 A metadata repository is a tool or suite of tools that allows users to store, manage, maintain and examine metadata.

7.3.3 Metadata is used by developers, analysts, designers, and database architects to provide them with information they need to architect and design effective solutions that meet the requirements for security, privacy, interoperability, semantic definition and vocabulary of the application.

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

8. REFERENCES

ADOA-P1000, Information Technology Policy

A.R.S. § 18-104

ADOA-P4440 – Data Governance Organizational Policy

9. ATTACHMENTS

None

10. REVISION HISTORY

Date	Change	Revision	Signature