P4400 DATA GOVERNANCE ORGANIZATION POLICY

DOCUMENT NUMBER:	**P4400**
EFFECTIVE DATE:	**JUNE 30, 2018**
REV:	**1.0**

1. AUTHORITY

To effectuate the mission and purposes of the Arizona Department of Administration (ADOA), the Agency 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, specified in P1000 Information Technology Policy and consistent with Statewide Information Technology policies and standards. Nothing in this policy shall be construed to supersede any Federal or State law, statute or rule.

2. PURPOSE

The purpose of this policy is to define controls to establish formal oversight of the people, processes and technologies that influence data throughout its life cycle, with the intent of reducing risk and improving outcomes of processes that depend on or use data. These controls will provide increased assurance that data is reliable, accurate, timely, fit for use, interoperable, consistent and protected from loss and unintended disclosure or alteration.

3. SCOPE AND APPLICABILITY

3.1 This policy applies to all employees and contractors within State Budget Units (BUs) 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 Applicability of this policy to third parties is governed by contractual agreements entered into between BUs and the third party. For contracts in force as of the effective date, subject matter experts (SMEs) acting under the guidance of the Data Policy Council (refer to section 6.1.1) should ascertain 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.

3.3 Applicability of this policy to specific information systems shall be determined by the Data Policy Council as defined below. Budget units may implement additional controls, roles or organizational structures as they deem necessary to suit their business or project needs.

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 Director, Commissioner, Executive Director or other Chief Executive Officer of the Agency (referred to herein as "Director") shall be responsible for ensuring the effective implementation of Information Technology Policies, Standards, and Procedures (PSPs) within the Agency.

5.2 Agency 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 policies, standards and procedures.

5.4 Subject Matter Experts (SMEs) shall ensure that this Policy is referenced in Project documents and that Parties are contractually obligated to follow this policy [DMM-DMS 3.5, 3.6].

5.5 The Data Policy Council (Sec 6.1.1) shall carry out the responsibilities defined in this Policy.

5.6 The Data Management Committee (Sec 6.1.2) shall carry out the responsibilities defined in this Policy.

5.7 Data Owners (Sec 6.1.3) shall carry out the responsibilities defined in this Policy.

5.8 Data Stewards (Sec 6.1.4) shall carry out the responsibilities defined in this Policy.

5.9 Data Custodians (Sec 6.1.5) shall carry out the responsibilities defined in this Policy.

6. POLICY

6.1 Each Agency shall establish the following oversight roles [DMM-DMF 2.3, 3.3]. If the size of the Agency does not warrant the creation of multiple roles, the Director at his or her discretion may combine roles to meet the business needs provided that the responsibilities defined below are designated to those roles:

6.1.1 Data Policy Council (DPC)

a) The Director or his/her designee shall appoint a DPC.
b) The DPC may include business and technology representatives from every Division within the Agency and at least one representative from the Data Management Committee of each Division.

c) The DPC shall be chaired by the Chief Data Officer if one has been appointed. If none has been appointed then the Director or designee shall appoint a chairperson. [CMMI-DEV-1.3-GP2.1][DMM-DMS 3.3].
d) The Data Policy Council shall undertake at a minimum the following responsibilities:
    i Designate Information Systems as Covered Information Systems (Sec 6.4);
    ii Ensure that data management objectives, priorities and scope are defined and approved and that they reflect agency business objectives [DMM-DMS 2.1, 2.2, 3.1, DMM-DMF 2.5, 3.3];
    iii Maintain and monitor compliance with data governance policies, standards and procedures [DMM-DMS 2.4, 3.7];
    iv Recommend solutions to issues relating to data governance;
    v Maintain a Center of Excellence for Data Governance as a resource where developers and stakeholders within the Budget Unit can find information about data governance policies, standards and procedures, best practices, tools, interpretations and training support [CMMI GP3.2] [DMM-COM 2.2, 3.1,3.3];
    vi Support the Data Management Committee(s);
    vii Collaborate with the DPCs and DMCs at other Budget Units to establish data governance and management on joint projects and initiatives;
    viii Provide for education, training and awareness of Data Governance within the Agency. [DMM-DMS 3.5, DMM-DMF 3.5]

6.1.2 Data Management Committee (DMC) - The Assistant Director of each Division (or equivalent) or his/her designee shall determine, with the assistance of the Data Policy Council, whether the Division needs a DMC, and, if so, the composition of the DMC. The DMC shall include one or more individuals representing the following roles [GP2.7]:

a) Data Architects;
b) Business Data Owners;
c) Data Stewards;
d) Enterprise Architects;
e) Database Administrators;
f) Infrastructure, especially storage architecture;
g) Security and networking.

6.1.3 The DMC shall undertake the following responsibilities:

a) Recommend, periodically review and monitor data governance policies, standards and procedures [GP2.6; GP3.1] [DMM-COM 2.2, 3.1, 3.3];

b) Establish and maintain Data Governance Procedures for the Division [CMMI GP2.2; GP3.1] [DMM-DMS 3.5, 3.4];
c) Maintain a knowledge base about Data Governance in the Division in alignment with the Center of Excellence [CMMI GP2.1-OT] [DMM-DMS 3.5];
d) Facilitate compliance with Data Governance Policies;
e) Define metrics to be used to measure and assess the achievement of objectives for data management. [DMM-DMS 2.5]
f) Train, advise and mentor staff on the Data Governance Policies, Standards and Procedures [CMMI GP2.1-OT];
g) Ensure that data policies, standards and procedures are considered in procurement documents, business requirements, technical design, project plans, budgets and operations plans and documents for all Information Systems [CMMI GP2.1-RD -REQM] [DMM-DMF-2.1];
h) Review and approve in a timely manner, Information System designs, architecture, requirements, release and operations plans received for compliance with Data Governance Policies, Standards and Procedures; [CMMI GP2.1-DAR –REQM –TS –CM; SP2.2; CM-SG1] [DMM-DMS 3.6, DMM-DMF2.2]];
i) Respond to and assist with resolving questions, conflicts and decisions about data; [CMMI GP2.1-OPD –OT -PPQA];
j) Undertake additional responsibilities as may be specified and authorized in the Policies, Standards and Procedures for Data Governance.
k) Meet and render decisions in a timely manner such that it does not impede the progress of any project.

6.1.4 Data Owners

The DPC shall designate a Data Owner for each Business Domain for the purpose of assigning decision-making authority and accountability for monitoring and enforcing policy. Examples of Business Domains are accounting, purchasing, procurement, asset management, case management or health care claims.

6.1.5 Data Owners shall undertake the following responsibilities:

a) Designate, train and monitor performance of the Data Stewards;
b) Establish and document business rules and a business glossary of terms relating to the data and communicate them to the Data Management Committee and other stakeholders;
c) Support the Data Policy Council;
d) Ensure that business requirements are established, documented and communicated;

e) Make and provide for the enforcement of all decisions about the data, including assigning authority to share, exchange, modify, define, delete and use the data. [CMMI GP2.7];
f) Designate at least one Data Steward for each Data Domain.

6.1.6 Data Stewards

a) Data Stewardship is the formalization of accountability for the management of data and data-related assets.
b) The Data Owners shall designate one or more Data Stewards. Depending on the budget unit's business needs there may be more than one level of data steward, at the Data Domain, Tactical or Operational levels.
c) Data Stewards may be assigned to data subdomains and to multiple data domains if warranted by the budget unit's business needs and approved by the Data Owner.
d) Data Stewards shall carry out their day-to-day processes and procedures in a manner that maintains data quality, usability and fitness for use. [GP2.7].
e) Performance measures and supervision of Data Stewards shall be put in place in accordance with industry best practices and Agency Procedures;
f) The Agency shall provide appropriate tools and training to designated Data Stewards to enable them to carry out their responsibilities effectively.
g) Data Stewards shall:
    i Be accountable to data owners for the quality of the data under their stewardship;
    ii Define data used by their job function, how the data will be used and how it will be managed;
    iii Produce, create, update, delete, retire or archive data;
    iv Maintain documentation and metadata.
    v Use data to perform their job functions and business processes;
    vi Create or review data definitions;
    vii Ensure that data is used within the established rules;
    viii Ensure integrity and quality of data is maintained;
    ix Communicate new and changed business requirements to impacted stakeholders;
    x Communicate concerns, issues and problems to those who can effect corrections; and
    xi Support and collaborate with other Stewards.
h) Data Owners may delegate the following additional responsibilities to one or more Data Domain Stewards:
    i Facilitate resolution of issues pertaining to their data domain;
    ii Responsible for enterprise level management of a data domain;

iii Initiate, facilitate and participate in cross-business unit resolution of data definition, production and usage issues;
iv Escalate documented issues to those who can effect corrections;
v Document data classification rules, compliance and business rules and ensure the rules are communicated to all stakeholders and data stewards in their domain; and
vi Participate in tactical groups with other Stewards and with the Data Management Committee to address and resolve issues and projects within their domain and business unit.
vii Communicate data policies, standards and procedures to other Stewards in their business unit, train them and ensure they understand the rules and risks;
viii Document and communicate issues pertaining to specific domains to the Domain Steward;
ix Work with Data Domain Stewards and Operational Stewards on specific tactical teams;
x Participate in the organization's change control process.

6.1.7 Data Custodians

a) A Data Custodian is person or group who has physical or operational control of a data repository. It includes, without limitation, roles such as database administrators, system or server administrators, backup operators and storage server administrators. A person need not be explicitly designated as a Data Custodian. If their duties with respect to a given data set include the foregoing responsibilities, they are implicitly deemed to be Data Custodians and have the responsibilities designated in this Policy.
b) A Data Custodian may have custody of data that belongs to the Agency, a customer or some other entity.
c) A Data Custodian is not a Data Owner unless explicitly designated as such.
d) Data Custodians are responsible and accountable for performing their duties with respect to data in their custody in accordance with Agency Policies, Standards and Procedures, the Policies, Standards and Procedures of the owner of that data and to such other Policies, Standards and Procedures as may be designated in an agreement between the Agency and the customer or owner.

6.2 Technology, tools and enablement. The Budget Unit shall:

a) Provide the technology and tools needed by the Data Owners, Data Management Committees and Data Stewards to carry out their responsibilities and shall train the Data Stewards on their usage. The purpose of these tools is to facilitate the definition, production and usage of data in a consistent manner

across the enterprise. Such tools may include data modeling, data classification, data profiling and quality metrics [CMMI GP2.3 –CAR –CM; GP2.5].;

b) Put procedures in place to ensure that best practices are enforced for the selection, design, implementation and management of systems that facilitate or automate the detection, prevention and correction of errors;
c) Ensure that the role of Data Steward is well understood within the organization; that Data Stewards are accountable for data under their stewardship and that Stewards are empowered to communicate effectively and drive change when needed to resolve and prevent issues, problems and errors with data;
d) Document the roles of the Data Steward, Data Management Committee and Data Owner in the Responsibility Assignment Matrix of a Project [CMMI GP 2.4]; and
e) Ensure that documentation is maintained and that cross-training is provided for all business-critical data management roles.

6.3 Training

6.3.1 Data Stewards shall receive specific training and be responsible for the following topics:

a) Awareness of the points at which their job functions have an impact on data definition, production and usage;
b) The business rules, policies and regulations surrounding the data they define, produce and use;
c) Awareness of the impact of failing to follow the business rules, policies and regulations;
d) The procedures for resolving errors, issues, problems that affect data; and
e) Awareness that they will be held accountable for following the business rules, policies and regulations.

6.3.2 Data Domain Stewards shall receive specific training covering all the topics of the Data Steward training plus the topics listed below.

a) Awareness of all the points at which their data domain impacts or is used by other business units;
b) Contact information and introductions to all Data Stewards within the budget unit and other business or budget units that impact their data domain;
c) Procedures for resolving issues, problems and errors that affect their data domain;
d) The use of enterprise data management tools including those for analyzing data quality, data modeling and data classification;

e) Strategic changes to data domains such as migration to new systems, databases, cloud servers, implementation of data warehouses, publication of data via services or API's, additional consumers of data from their domain, master data management and all similar initiatives that may have an impact on the data domain;

6.3.3 Training required by this policy shall be given at the time of hiring or on-boarding of employees or contractors. Training shall be repeated when significant changes are made to systems, procedures or job functions. If no such changes are made within a given year, refresher training shall be repeated annually during a month to be designated by the Budget Unit.

6.4 Whenever a position or role impacts the definition, production or usage of data the employee, contractor or service provider shall be informed that they will be held accountable for the quality of that data. Personnel evaluation procedures and instruments shall measure and provide feedback on the performance of data stewardship responsibilities and may specify corrective actions if performance is substandard.

6.5 The Data Policy Council shall review all Information Systems in use within the Agency, whether developed internally or by contracted parties or acquired as off-the-shelf software, with or without modifications, from third parties and determine whether each Information System shall be covered by the Data Governance Policies. Each Information System designated as such by the DPC shall be referred to as a Covered Information System (CIS). The DPC shall use the following minimum guidelines in determining whether a particular entity should be designated as a CIS:

6.5.1 Information Systems procured, specified, implemented, developed, acquired or undergoing modifications, enhancements or upgrades after the effective date are CIS when one or more of the following is true:

a) The cost of the Information System exceeds $1,000,000;
b) The Information System provides a critical business function;
c) The Information System provides data or data services to external applications or systems;
d) The Information System consumes data or data services from external applications or systems;
e) The data includes sensitive, private or confidential data as defined in Statewide Policy P8110 or Statewide Standard S7410 – Classification of Data;
f) The data is published for consumption by the public;
g) A process to access the data exists or is being developed and requires a level of security equivalent to SICAM Assurance Model Level 2 or higher. (See NIST Special Publication 800-63).

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

6.7 Third parties supplying Information Systems to the Agency, developing information systems on behalf of the Agency or providing Information System related services to the Agency shall be required to comply with this Policy.

7. DEFINITIONS AND ABBREVIATIONS

7.1 Data stores, applications, information systems and data exchanges are all designated as Information Systems for the purposes of this Policy.

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

8. REFERENCES

8.1 P1000 Information Technology Policy

8.2 P7000 Enterprise Architecture Policy

8.3 P8001 IT Security Policies

8.4 CMMI for Development, Version 1.3 (CMMI References)

8.5 Data Management Maturity Model V 1.0 (DMM References)

8.6 NIST Special Publication 800-63

9. ATTACHMENTS

None.

10. REVISION HISTORY

Date	Change	Revision	Signature