| ARIZONA DEPARTMENT OF ADMINISTRATION | **Statewide**<br>**POLICY** | **State of Arizona** |
|---|---|---|

# P4460 DATA GOVERNANCE DATA QUALITY POLICY

| | |
|---|---|
| **DOCUMENT NUMBER:** | **P4460** |
| **EFFECTIVE DATE:** | **NOVEMBER 1, 2020** |
| **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 or statute.

## 2. PURPOSE

The purpose of this policy is to provide guidance and best practices for the implementation of measures to improve and maintain Data Quality by Budget Units.

## 3. SCOPE AND APPLICABILITY

**3.1** This policy applies to all employees and contractors within State Budget Units, Agencies, Boards and Commissions (referred to herein as "Budget Unit" or "BU") who work with data or repositories of data while executing business functions, activities or services for or on behalf of the BU, its Divisions or its customers.

**3.2** This policy applies to all Covered Information Systems designated as such by the Data Policy Council of the BU. A BI system that is used for reports, dashboards and analysis of a Covered Information System may be designated as a Covered BI System for the purposes of this Policy.

**3.3** Applicability of specific standards issued under this policy shall be as specified in those standards, and may either be extended or reduced by those standards.

**3.4** An Information System that contains data classified as Private shall be considered a Covered Information System regardless of whether it has been formally designated as such by the Data Policy Council.

**3.5** Applicability of this policy to third parties is governed by contractual agreements entered into between ADOA 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.

**3.6** 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 then procedures to keep them compliant for the remainder of their lifetime shall be implemented or continued.

**3.7** 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.

**3.8** State Agencies and Third parties supplying information systems to ADOA or developing information systems on behalf of ADOA shall be required to comply with this Policy including documentation to demonstrate compliance with all State policies and documented security controls.

## 4. EXCEPTIONS

All requests for exceptions to this policy shall be submitted in writing to the State Data Management Architect (SDMA) stating the reasons for the exception, impact, risk and alternate controls that will be implemented to minimize impact and risk. The SDMA shall assess the request and make a recommendation to the Chief Information Officer. Exceptions will be granted only upon approval by the Chief Information Officer or designee.

## 5. ROLES AND RESPONSIBILITIES

**5.1** The Director, Commissioner, Executive Director or other Chief Executive Officer of the BU (referred to herein as "Director") shall be responsible for ensuring 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 policies, standards and procedures.

**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.

**5.5** The Data Owners (Data Domain Stewards) shall designate which BI systems are considered Covered BI Systems for the purpose of this policy.

## 6. POLICY

**6.1** The Policy Statements below are based on the CMMI Data Management Maturity Model (DMM). The references in each section are numbered according to capability levels they represent in the DMM. 1.x – Capability level 1; 2.x – Capability Level 2; 3.x – Capability level 3. See Annex "A" for a description of the levels.

**6.2** Data Quality Strategy (DQS) – BUs require an integrated, organization-wide strategy to achieve and maintain the level of data quality required to support the BU's business goals and objectives. [DMM:DQS]

**6.3** BUs shall establish a Data Quality Strategy which includes quality goals and objectives, business benefits, implementation priorities, quality criteria, policies and governance, a data profiling strategy and an implementation plan.

6.3.1 BUs shall document their data quality objectives, rules and criteria, with the participation of business stakeholders, and a process shall be put in place to ensure that plans are followed, rules are implemented and criteria are monitored [DMM:DQS 1.1, 1.2, 1.3]

6.3.2 The data quality strategy should be created with the participation of business stakeholders with reference to business objectives and plans, and should be approved by executive management [DMM:DQS 2.1, 2.2, 2.5];

6.3.3 The data quality strategy should be followed across the entire organization and supported by policies, processes, guidelines and training [DMM:DQS 2.3, 3.1].

6.3.4 The data quality strategy should refer to the data quality dimensions selected by the BUs stakeholders and the Data Policy Council [DMM:DQS 2.4].

6.3.5 The data quality strategy shall be reviewed periodically to ensure that it continues to meet business needs. [DMM:DQS 3.5]

6.3.6 Data quality strategy should be supported by defined personnel roles and responsibilities for governance, implementation and ongoing management of the data quality procedures. [DMM:DQS 3.2]

6.3.7 Policies, processes and governance should apply to each phase of the data lifecycle. [DMM:DQS 3.4]

6.3.8 Data quality projects such as profiling, assessments, cleansing and risk assessments should be aligned with the business needs defined in the data quality strategy. [DMM:DQS 3.6; DP 2.2, 3.1, 3.2, 3.4; DQA 2.1, 2.5, 3.1, 3.2; DC 2.1, 2.5, 3.2]

**6.4** Data Profiling – Data Profiling reveals what is stored in a database and how physical values align with expected allowed values as listed in metadata repositories and other documentation. Profiling examines values, ranges, frequency distribution of data values and whether data values adhere to business rules. [DMM:DP]

- 6.4.1 BUs shall establish a data profiling methodology and approach. [DMM:DP 2.1, 3.1]
- 6.4.2 Projects should include a data profiling plan that is shared with stakeholders, including the project and data governance teams. Results from data profiling should be reported to the same stakeholders. [DMM:DP 2.2, 2.3, 2.5]
- 6.4.3 Methodologies, practices, tools and results templates should be defined and standardized across the organization. [DMM:DP 3.1]
- 6.4.4 Profiling processes should be usable across the enterprise with multiple data stores. [DMM:DP 3.5]

**6.5** Data Quality Assessment – Data Quality Assessment [DMM-DQA] provides a systematic approach to measure and evaluate data quality on multiple dimensions in accordance with a set of data quality rules.

- 6.5.1 BUs shall determine which data elements are deemed critical to an organization and establish procedures for periodic, systematic assessment of the quality of those elements. [DMM:DQA 2.1, 2.3, 3.1]
- 6.5.2 Data quality assessments should include recommendations for remediation of defects. [DMM:DQA 2.4]
- 6.5.3 Data defects should be resolved through a root cause analysis of the source of the defect and remediation of the process that caused the defect. [DMM:DQA 2.5, 3.3, 3.5]
- 6.5.4 BUs should establish a process for assessing the business impact of data defects and, using that information, determine the priority, risks and costs of fixing the defects. [DMM:DQA 2.5, 3.2]
- 6.5.5 Data quality should be assessed according to thresholds and quality targets for each quality dimension. [DMM:DQA 2.1, 3.4]

**6.6** Data Cleansing is the practice of correcting data according to predefined business rules.

- 6.6.1 Data Cleansing strategy, scope and requirements should be clearly defined and communicated across the organization. [DMM:DC 1.1, 2.1, 2.3, 2.5]
- 6.6.2 Data Cleansing processes should be defined and planned. [DMM:DC 2.4, 2.6]
- 6.6.3 Data Cleansing scope and plan should conform to data quality requirements established by the business stakeholders. [DMM:DC 2.2]
- 6.6.4 Data changes should be communicated to the stakeholders and resolved at the source. [DMM:DC 2.7. 3.2]
- 6.6.5 Data cleansing activities should be performed in a manner that preserves and documents changes to the data. [DMM:DC 3.1]
- 6.6.6 Data cleansing results and reports should be shared across the organization. [DMM:DC 3.5]

6.6.7 Data cleansing rules should be established and monitored by the Data Policy Council and should be applied consistently across the organization. [DMM:DC 3.3, 3.4]

## 7. DEFINITIONS AND ABBREVIATIONS

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

## 8. REFERENCES

**8.1** P1000 – Information Technology Policy

**8.2** A.R.S. § 18-104

**8.3** P4400 – Data Governance Organization Policy

**8.4** S7410 – Data Classification Standard

**8.5** DMM refers to the CMMI Data Management Maturity Model version 1.1 topics DQS: Data Quality Strategy; DQA: Data Quality Assessment; DP: Data profiling; DC: Data Cleansing. A copy of the full DMM is available at https://drive.google.com/file/d/1OAHf1KZdTLSF3ngq6urpxEkbCylHvUPh/view

## 9. IMPLEMENTATION GUIDELINES

BUs should begin a phased implementation of this policy on the following timeline. BUs that already have capabilities in place should accelerate the implementation based on business needs.

- February 1, 2021 – Submit an implementation plan for review by ADOA-ASET.
- July 1, 2021 – Commence implementation of the Level 1 capabilities.
- January 1, 2022 – Commence implementation of Level 2 capabilities.
- January 1, 2023 – Commence implementation of Level 3 capabilities.

## 10. ATTACHMENTS

Data Management Maturity Model version 1.1

Data Quality Policy Implementation Plan Template

## 11. REVISION HISTORY

| Date | Change | Rev | Signature |
|---|---|---|---|
| **12/17/2018** | Initial straw-man drafted | 0.1 | Jeff Wolkove |
| **4/9/2020** | Review, update & revisions by Data Policy Work Group | 0.2 | Jeff Wolkove |
| **10/22/2020** | Final revisions to put policy in force and add references | 1.0 | Jeff Wolkove |

Approved by the State Chief Information Officer

Effective date: November 1, 2020

Date approved: Oct 22, 2020

By: JR Sloan, State CIO

Signature: