P4450 DATA GOVERNANCE DATA OPERATIONS POLICY

DOCUMENT NUMBER:	**P4450**
EFFECTIVE DATE:	**JANUARY 1, 2021**
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 for data operations, including:

2.1 Implementation, operations and change management of Business Intelligence (BI) tools;

2.2 A framework for establishing business processes that ensure that BI produces consistent, high quality, actionable and reliable information;

2.3 Controls over manual changes to database contents;

2.4 Controls over data retention.

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 Chief Information Officer stating the reasons for the exception, impact, risk and alternate controls that will be implemented to minimize impact and risk. 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.

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 Business Intelligence – Definition & Background

Business Intelligence (BI) in the context of this Policy refers to the process of analyzing data and producing reports, data extracts, charts, dashboards and similar output, referred to generically as BI Reports, and to the software and infrastructure elements that support the BI function.

The usability of BI Reports is dependent upon many factors including accuracy, timeliness, availability, change management, service level compliance and the underlying data.

The dependency upon underlying data (BI Source Data) includes factors such as its fitness for use, accuracy, timeliness, completeness, security, stability and stewardship, together with transparent communication to consumers of BI Reports when any of these is compromised.

6.2 The Data Management Committee shall undertake the following responsibilities with respect to Covered BI Systems:

6.2.1 Review and approve technical plans for views and other queries to be executed against a database;

6.2.2 Ensure that BI systems can establish data connections to third-party SaaS applications and that data models are available to analysts.

6.2.3 Act as final decision maker on all matters impacting the access to BI Source Data, and provide for the implementation of those decisions. These matters may include without limitation:

a) Determining whether the source data for a BI Report should be a production database or if a separate repository, data mart or warehouse is needed;
b) Establishing business processes to maintain the BI Source Data;
c) Supporting the Data Stewards of the BI Source Data.

6.2.4 Support a healthy BI environment which may include the following practices:

a) Plan for needed infrastructure resources;
b) Assess opportunities to optimize the DB for the underlying queries;
c) Assess the use of and need for new indexes;
d) Plan for periodic or more frequent index rebuilds;
e) Plan to create and monitor slow query logs;
f) Monitor performance changes;
g) Determine whether a view or underlying functions should be in a stored procedure or a materialized view in the database;
h) Respond timely to database issues, problems and adverse events.

6.3 BI Availability

6.3.1 BI Systems including all components shall be managed to a service level that meets the business needs of the BU. Availability is defined as the percentage of time that a BI System is operational, the BI Reports are accessible to users and business processes that rely on them, and business processes that maintain the BI Source Data are able to run successfully. Availability calculations exclude service outages that have been properly planned, approved and communicated in advance.

6.3.2 Any of the following events will render a BI System unavailable for the purposes of this Policy:

a) The BI System or user interface fails to respond to requests within the acceptable response time. The acceptable Response Time shall be defined for the BI System at the time of implementation;
b) Some, most or all of the BI Source Data is inaccessible for any reason;
c) Late or failed Extract-Transform-Load (ETL) processes or data exchanges that the BI System is dependent upon.

6.4 Change management

6.4.1 Changes to software, hardware, network, infrastructure, co-located applications, reporting platforms, database schemas, views and indexes are examples of areas where changes can trigger unexpected and adverse changes in reports, applications and data exports. The Data Domain Steward, DMC and database administrators shall be consulted in advance of such changes, analyze and report on potential risks and participate in the change process to the extent necessary to avoid and minimize the impact of adverse outcomes.

6.4.2 Changes to BI views, database schemas, stored procedures and other properties of the BI Source Data may adversely impact existing reports. Production views used in reports shall not be modified in place. They shall instead be copied or cloned to create new views that satisfy the business need.

6.5 Database access and manual changes

6.5.1 The entry and update of data stored in databases in the normal course of business shall be accomplished via the business applications that implement the business rules and input edits that protect data from unauthorized or accidental access, unauthorized changes and ensure security, integrity, and accuracy of the data.

6.5.2 Data entry and update using direct database access SQL statements (Manual Changes) shall be permitted only by written permission of the Data Management Committee and the Data Owner and access rights shall be managed in accordance with Security Policies.

6.5.3 Agencies shall provide and maintain documented procedures to ensure that manual changes to the data are documented, approved, implemented and validated and that an audit trail is maintained. Such procedures shall include a requirement that each update requires approval by a Data Owner or their delegate and that all personnel involved in the process are trained.

6.5.4 Permission for read-only database access for ad-hoc queries, reporting and analytics shall be granted only by written permission of the Data Management Committee and the Data Owner. The Data Management Committee shall ensure that access to production databases for these purposes will not interfere with production service levels at any time.

6.5.5 Agencies shall provide appropriate training to all individuals granted read-only or update permissions on Covered Databases which shall encompass the classification of the data they have access to and any relevant statutory obligations such as those regarding the treatment of Personally Identifiable Information and Personal Health Information.

6.6 Data Retention - In order to adhere to data retention requirements based on applicable law and the requirements set forth by the State Library and Archives (SLAPR), Data Domain Stewards in conjunction with Data Custodians shall:

6.6.1 Ensure that system requirements include a process for managing retention periods for the specific types of data stored by the application.

6.6.2 Establish processes, including, if appropriate, automated processes to purge data after the retention period;

6.6.3 Establish processes to mark data that should be retained beyond the statutory retention period, for example, data related to ongoing litigation, so it is not purged.

6.6.4 Review the data retention policies every two (2) years and make recommendations to Arizona State Library, Archives and Public Records (SLAPR) when changes are needed.

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 Data Management Maturity Model © 2014 CMMI Institute

8.3 A.R.S. § 18-104

8.4 P4400 – Data Governance Organization Policy

8.5 P8000 *et seq* – IT Security Policies

9. ATTACHMENTS

None.

10. REVISION HISTORY

Date	Change	Rev	Signature
12/17/2018	Initial draft finalized by Data Management Policy Committee	0.1	Jeff Wolkove
3/23/2020	Finalized by State Data Management Steering Committee and signed by the State Chief Information Officer	1.0	Jeff Wolkove

11. APPROVAL

I hereby approve this policy to be put in force as of January 1, 2021.

By: J.R. Sloan, State Chief Information Officer

Signature 

Date Apr 7, 2020