# P4430 DATA GOVERNANCE TECHNOLOGY POLICY

| | |
|---|---|
| **DOCUMENT NUMBER:** | **P4430** |
| **EFFECTIVE DATE:** | **JUNE 30, 2019** |
| **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. This Policy shall not be construed to supersede any federal and state statutes or rules related to data governance.

## 2. PURPOSE

This Policy establishes governance over the technical implementation of databases and the software and applications that interact with them to reduce risk, maximize interoperability and ensure that systems are developed and maintained in accordance with Statewide and Budget Unit (BU) strategic plans.

## 3. SCOPE AND APPLICABILITY

**3.1** This policy applies to all employees and contractors within State 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** This policy applies to all Covered Information Systems designated as such by the Data Policy Council of the BU.

**3.3** 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 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.

**3.4** 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.

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

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

**3.7** This policy does not apply to unstructured data repositories such as 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 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 users are appropriately trained and educated on Data Governance policies and shall monitor employee activities to ensure compliance.

**5.3** Individual Users shall adhere to all state and ADOA 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.

## 6. POLICY

**6.1** Systems, technologies, products and tools, including open source products, shall be classified into four categories:

**6.1.1** Strategic technologies are the currently acceptable platforms that fit the strategic goals of the BU and the State;

**6.1.2** Emerging technologies are new platforms that may be evaluated and considered for limited production use but are not yet considered Strategic due to risk, interoperability or other factors;

**6.1.3** Transitional and contained technologies are those platforms that are approaching end-of-life or end-of-support, have been superseded by more current technology or no longer meet the needs of the State and will be phased out at end of life. Implementation of new applications on these platforms is strongly discouraged;

**6.1.4** Rejected and obsolete technologies are no longer acceptable for use by the BU due to their cost, lack of support, maintainability, lack of skilled technicians, lack of reliable supporting infrastructure or other risk factors.

**6.1.5** Notwithstanding a product's classification, a product can only be used in new production, mission-critical or strategically important applications if

a) It is actively maintained by the manufacturer;
b) It is covered under a commercial support arrangement;
c) It is supported by the Budget Unit's enterprise technical support team.

**6.1.6** Databases residing on a desktop or laptop computer shall not be used in mission critical or strategically important applications.

**6.2** Database Availability

**6.2.1** Covered Databases shall be managed to a minimum service level of 99.99% availability unless there is a service level agreement or contract in place that allows a different availability level for a specific database or application. Availability is defined as the percentage of time that a Database is operational and the data in it is accessible to users and business processes that rely on it. Availability calculations exclude service outages that have been properly planned, approved and communicated in advance.

**6.2.2** The following events would render a database unavailable for the purposes of this Policy:

a) The database fails to respond to normal requests within a specified Response Time. The acceptable Response Time shall be defined for each application on a case-by-case basis at the time of implementation and shall be communicated to the Data Management Committee;

b) Some, most or all of the data in the database is inaccessible due to data corruption, connection failure, a malicious act, an improperly executed change or some other reason;
c) The database is inaccessible due to a network or other infrastructure failure, the server or the hardware it resides on was unexpectedly shut down or some critical failure has occurred where the database resides;
d) A database that is being restored following an outage, data corruption or other cause is considered unavailable until the restoration process completes.

**6.3** The following actions shall be taken on databases to ensure maximum availability and reduce risks of a database becoming unavailable. Actions required for a given Covered Database will be implemented on a case-by-case basis after these Policies are considered and the decisions to implement them in whole or in part are documented and approved by the Data Owner and the Data Management Committee.

**6.3.1** Backups of the database shall be made at regular intervals. Details and procedures shall be reviewed periodically with Data Owners, the Data Policy Council and business leaders to ensure they meet and continue to meet the business requirements. The frequency of this review shall be determined by the Data Policy Council. It is recommended that this review take place quarterly in the two years following implementation of a new application and at least annually thereafter. This review shall include the following factors:

a) Backup frequency and methodology should be sufficient to ensure recovery of all or substantially all of the data up to the moment of the failure, loss or corruption of data;
b) Ensure that estimated time for recovery of a full backup continues to meet business needs. BUs should consider that time to recover will depend on the size of the backup, steps required to obtain the storage media, load and validate it. Additional time may be needed to obtain, install and configure the infrastructure needed by the Database server;
c) Ensure that projected loss of transactions meets the business needs and that both IT and business procedures are in place to measure and mitigate this loss. BUs should consider that loss of data may depend on factors such as transaction or data integration velocity, frequency of backups;
d) Ensure that the availability and cost of alternative infrastructure on which to restore the backups and the application in the event of physical damage to the hardware continues to meet the business needs;
e) Ensure that disaster and unplanned outage recovery procedures and timelines continue to meet the business needs and that contingent funding is available;

f) Ensure that estimated time to repair and recover defective storage media continues to meet the business needs.

**6.3.2** Database high-availability options shall be used to provide a standby copy of a Database in the event that backups are insufficient to meet the business needs. These options maintain one or more up-to-date copies of the database in near real time;

a) Procedures to recover from an outage by connecting the applications to the replica shall be documented;
b) Replicas may be hosted in the same data center as the master, at a remote location, or both, depending on business continuity requirements.

**6.3.3** Storage

a) Covered Databases shall be stored on fault-tolerant media such as Storage Array Network (SAN) or RAID systems allowing rapid repair and recovery of the data on a faulty disk drive. Estimated time to recover shall be considered in the context of the business needs;
b) Storage devices shall be monitored for errors, slow performance and adequate space. Procedures shall be put in place to prevent and avoid any issues that might impact the service level.

**6.3.4** Performance monitoring

Appropriate tools and procedures shall be used to monitor databases, provide notifications and remediate performance issues that may arise out of unexpected outages, usage patterns, work load, unexpected change impacts, slow queries, access by reporting tools, malicious activities and long-running processes.

**6.3.5** Change management

Changes to software, hardware, network, infrastructure, co-located applications, reporting platforms, database schemas and indexes are examples of areas where changes can trigger database outages. The Data Management Committee 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** Data Architecture - Responsibility for Data Architecture shall be vested in the Data Management Committee (DMC).

**6.4.1** The DMC will have the following responsibilities with regards to Data Architecture:

a) Establishing and approving naming conventions for fields, tables, databases, stored procedures, functions and other objects in the database;
b) Exploring and approving the use of database management platforms including RDBMS and NoSQL platforms;
c) Establishing and approving standards including naming conventions, triggers and technical specifications of data elements, as required or appropriate for the application;
d) Consulting on and approving the design of physical database, tables, fields, data types, relationships and indexes required or requested by developers;
e) Approving the use of and establishing security around triggers, stored procedures, functions and scheduled database processes;
f) Architecting the physical layout of database artifacts on the infrastructure including the use of and balancing of partitions, table space, log files and other physical attributes impacting database storage, CPU capacity, network bandwidth and memory sizing of the server;
g) Ensuring that the data architecture is well documented and the documentation is maintained;
h) Ensuring that other Data Architecture best practices are followed in the implementation of a Covered Database or Covered Information System;
i) The DMC shall conduct its work in a manner that does not cause delays in the system development life cycle. The DMC may authorize team members to perform tasks related to data architecture that conform to established standards.

**6.5** Public Cloud Databases - Public Cloud databases include databases residing in a virtual server owned and managed by a BU and hosted by a public virtual infrastructure Cloud Provider or any database service offered by a Platform as a Service provider.

**6.5.1** Databases may be maintained in or migrated to Public Cloud facilities provided that the DMC has given approval after considering the following minimum requirements and reviewing the results of tests conducted to ensure they comply:

a) Usage charges, such as transaction and bandwidth charges, if any are levied by the Cloud Service Provider (CSP), shall be estimated based on existing transaction volume in the legacy infrastructure, or if unknown, based on estimates derived from physical characteristics of the database. Actual transaction charges shall be monitored closely following implementation to identify and avoid unexpected costs, and the DMC shall establish thresholds and ensure that automated alerts are in place when charges exceed those thresholds;

b) Sizing of the virtual infrastructure shall be sufficient to bear the work load of the database while maintaining availability service levels defined in this Policy or in separate service level agreements;
c) Security of the virtual server shall meet the security needs of the application and shall adhere to all applicable security policies;
d) Data access latency between the virtual infrastructure and the application that consumes the data shall be monitored and maintained within the required service levels defined in this Policy or in separate service level agreements;
e) Performance monitoring shall be provided either by the vendor or by using BU-provided tools.
f) The DMC and/or DBAs shall be given adequate access and control over tuning the database performance, resizing the server, and managing storage space as needed to maintain the service levels defined in this Policy or in separate service level agreements;
g) Disaster recovery, backup and replication processes that meet the business needs of the BU shall be put in place or remain in place in the virtual environment;
h) Procedures shall be in place to ensure that there is no loss of data or change in the precision, quality or usability of the data after migration to a cloud database.

**6.6** Protection of Confidential Data

**6.6.1** Data shall be protected in accordance with the Protections referenced in Policy 8350 – System and Communications Protections:

a) Cryptographic Services
b) Key Protection
c) Key Management Process
d) Public Key Infrastructure Certificates

**6.6.2** Data shall be encrypted according to the Acceptable Encryption Algorithms referenced in Standard 8350: System and Communication Protection Standard

a) Acceptable Security Strength
b) Symmetric Encryption Algorithms
c) Key Agreement Schemes
d) Hash Functions
e) Digital Signature Algorithms
f) Message Authentication Codes

**6.6.3** Data shall retain its Security Classifications as it traverses any physical or logical boundary such as a Division, computing or storage device, network or software

application system and appropriate measures for securing that data shall be implemented at each stage.

## 7. DEFINITIONS AND ABBREVIATIONS

**7.1** The data repository of a Covered Information System is considered a Covered Database 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** A.R.S. § 18-104

**8.3** P7000 - Enterprise Architecture Policy

**8.4** P4400 – Data Governance Organization Policy

**8.5** P8000 - IT Security Policy

**8.6** S8100, Account Management Standard

## 9. ATTACHMENTS

None.

## 10. REVISION HISTORY

| Date | Change | Revision | Signature |
|---|---|---|---|
| | | | |