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

P4465 STATE-OWNED CLOUD DATA POLICY

DOCUMENT NUMBER:	**P4465**
EFFECTIVE DATE:	**NOVEMBER 1, 2020**
REVISION:	**1.0**

1. AUTHORITY

To effectuate the mission and purposes of the Arizona Department of Administration (the "Department"), the Department shall maintain a coordinated statewide plan for information technology (IT) implemented and maintained through policies, and adoption of statewide technical, coordination and security standards as authorized by Arizona Revised Statute (A.R.S.) § 18-104. Formulate policies, plans and programs to effectuate the government information technology purposes of the department.

2. PURPOSE

The purpose of this policy is to provide guidance and best practices for the implementation of measures to ensure that the State and its Budget Units maintain ownership of State Data in the custody of vendors and other third parties.

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 Business Intelligence (BI) system that is used for reports, dashboards and analysis of a Covered Information System may be designated as a Covered 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 BUs and the third party. For contracts in force as of the effective date, subject matter experts (SMEs) acting under direction of the BU's Data Governance Council and/or Data Domain Stewards, in coordination and consultation with the appropriate agency chief procurement officer, 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 work with the relevant procurement officer to 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 the appropriate section of state contracts that specify the business and technical specifications of Information Systems being developed, procured or acquired, as needed.

3.8 State Agencies and Third parties supplying information systems to a BU 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.

4. EXCEPTIONS

All requests for exceptions to this policy shall be submitted in writing to the State CIO 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 Governance 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 systems are considered Covered Systems for the purpose of this policy.

5.6 As needed, coordinate with the State Procurement Office or relevant procurement officer with regard to any issues related to contract amendments, contract management, new solicitations, or contractor issues.

6. POLICY

6.1 As the State migrates more applications to third party solutions commonly referred to as "Software as a Service", "Platform as a Service" or "Infrastructure as a Service", we encounter a wide variety of terms, conditions and restrictions regarding access to data stored in these systems. This data will be generically referred to in this Policy as "Cloud Data". This document establishes one policy for the terms and conditions relating to Cloud Data.

6.2 All contracts with third parties that involve the storage and maintenance of Cloud Data shall include language that substantially gives effect to the following principles, namely:

6.2.1 Cloud Data is, and shall always remain the property of the State.

6.2.2 There shall be a provision in state contracts that allows the State's access to Cloud Data by an appropriate and mutually agreeable means such as, extracting data in whole or in part, connecting directly to the Cloud Data physical data store or a copy of it, accessing an Application Programming Interface (API) to access the data, or making use of the Data in a data warehouse or other repository.

6.2.3 Costs, if any, for accessing Cloud Data shall be included in the contract price. The cost of accessing Cloud Data shall form an integral part of the cost of the related application. If a specific format is required to transition Cloud Data back to the State, any costs associated with that transition shall be included in the contract price as well. BUs shall ensure that such costs are built into their budget for the related application and shall not restrict access to Cloud Data by reason of the cost of accessing it.

6.2.4 All contracts with third parties that involve the storage and maintenance of Cloud Data shall include provisions that allow the State sufficient access to the vendor's Data Model to allow the State to understand and utilize the Cloud Data for analytical purposes.

6.2.5 The existence of "Embedded Analytics" in the vendor's solution does not in and of itself, provide sufficient reason to restrict access to Cloud Data, and in such cases, the rights of the State to extract data, store it in its own Data Warehouse(s) and utilize it without restriction shall not be diminished.

6.2.6 The existence of contractor intellectual property and/or contractor proprietary processes in the contractor's Data Model does not, in and of

itself, provide sufficient reason to restrict access to Cloud Data, and in such cases, the rights of the State to extract data, store it in its own Data Warehouse(s) and utilize it without restriction shall not be diminished.

6.2.7 There shall be no cost associated with extracting and transferring Cloud Data to the State upon termination of a contract, unless the State and contractor have negotiated for the extraction and transfer of Cloud Data for a specific price in a mutually agreed-upon contract term.

6.2.8 Contracts shall include language that governs the disposition of data upon termination of the contract, which is in compliance with state record retention policies set by the Arizona State Library, Archives & Records.

6.2.9 Contracts shall include language that specifies that the vendor cannot access, use, sell, provide access to, distribute or disclose State Cloud Data to affiliates, subsidiaries or third parties without written consent.

7. DEFINITIONS AND ABBREVIATIONS

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

7.2 Cloud Data means all information, whether in oral, written, or electronic form, created by or in any way originating with the State, and all information that is derived from any computer processing, or other electronic manipulation, of any information that was created by or that in any way originated with the State, in the course of using and configuring the Cloud Services.

8. REFERENCES

8.1 P1000 – Information Technology Policy

8.2 A.R.S. § 18-104

8.3 P4400 – Data Governance Organization Policy

9. ATTACHMENTS

None.

10. RESOURCES

10.1 Indiana procurement code has a standard template for procurement of SaaS, PaaS, IaaS at https://www.in.gov/idoa/3000.htm

10.2 Kentucky has standard terms and conditions for cloud service RFPs reproduced at https://docs.google.com/document/d/1KNcxf7YGTbKoZFu3Qi2XZxkVykPLL8miglp1LQs5QjA

10.3 Wyoming is developing standard T&Cs for RFPs including one for metadata, reproduced at https://docs.google.com/document/d/1yGw18SRGEz-DLOVwx11oXaWEORWRdNQplSFrjZdgeJ0

10.4 Oregon has a statute that includes a requirement that all new tech procurements submit a data dictionary to the State Chief Data Officer, along with requirements that new technologies cannot prohibit access to data. https://www.oregonlaws.org/ors/276A.365

11. REVISION HISTORY

Date	Change	Rev	Name
01/28/2020	Initial straw-man drafted	0.1	Jeff Wolkove
09/10/2020	Added suggested revisions	0.2	Jeff Wolkove
10/27/2020	Approved	1.0	Jeff Wolkove

Approved by the State Chief Information Officer

Effective date: November 1, 2020

Date approved: Nov 16, 2020

By: JR Sloan, State CIO

Signature: