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

P1100 - CLOUD SMART POLICY

DOCUMENT NUMBER:	P1100
EFFECTIVE DATE:	9/6/2023
VERSION:	2.0

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" implemented and maintained through policies, and "adopting statewide technical, coordination and security standards" as authorized by Arizona Revised Statute A.R.S. § 18-104 (A)(1)(a). The Department shall also "formulate policies, plans and programs to effectuate the government information technology purposes of the department" pursuant to A.R.S. § 18-104 (A)(13).

2. PURPOSE

The purpose of this policy is to provide a consistent management approach to development of policies, standards and procedures (PSPs). Information Technology (IT) PSPs are essential elements of the application, implementation, and operation of IT systems. The purpose of this policy (Policy) is to outline the use of cloud technologies for all infrastructure, platform and software purchases by all Budget Units (BUs) covered by this policy in the State of Arizona (the "State"). The goal is to promote and encourage the appropriate use of cloud technologies by the BUs.

This policy establishes standards to ensure that state agencies:

2.1. Appropriately analyze and document the benefits, costs, and risks to the state before contracting for a Cloud, Hosted Service or other platform.

2.2. Assess the readiness of a Cloud, Hosted Service Provider, or other platform to deliver a solution that meets the state's requirements.

2.3. Conduct planning to ensure that state information and financial assets are appropriately protected when adopting a Cloud, Hosted Service or other platform.

2.4. Assist BUs to realize the full benefit of cloud technology by cultivating an organizational mindset of constant improvement and learning.

3. SCOPE

This policy applies to all Budget Units, as defined in A.R.S. § 18-101, and IT integrations and/or data exchange with third parties that perform IT functions, activities or services for or on behalf of Budget Units. Applicability of this policy to third parties is governed by contractual agreements entered into between Budget Units and the third party/parties. In addition, PSPs for security technology are covered by Policy 8120: Information Security Program.

4. EXCEPTIONS

4.1. If a BU needs an exception from any of the requirements in this Policy, they must request and obtain approval from the State Chief Information Officer (CIO). If approved, the exception is allowed for up to 24 months. At the expiration of the exception term, the BU must reassess any gaps and seek a new exception from the CIO.

5. ROLES AND RESPONSIBILITIES

5.1. State Chief Information Officer (CIO) or his/her designee shall:

5.1.1. Be subject to the requirements of the Arizona Procurement Code and be ultimately responsible for reviewing and approving vendors that provide cloud solutions including infrastructure, platforms and software.

5.1.2. Review and approve/deny BU requests for exceptions to this Policy.

5.1.3. Be responsible for establishing an internal Statewide Cloud Center of Excellence and Cloud Advisory Council to include multiple business units and technical teams from State agencies.

5.2. State Chief Information Security Officer (CISO) shall:

5.2.1. Advise the State CIO on any/all cloud infrastructures, platforms and software that meet the State security policies.

5.2.2. Review and ensure that cloud vendors meet or exceed all required State security controls as specified by policy.

5.3. Agency CIO or his/her designee shall:

5.3.1. Promote efforts within the BU to establish and maintain appropriate and effective use of cloud systems and their alternatives going forward.

5.3.2. Ensure that the State security policies are met by the BU and its cloud vendors. Including those PSPs for security technology such as Policy 8120: Information Security Program.

5.3.3. Be responsible for following and developing their cloud and security maturity levels.

6. POLICY

6.1. Each BU should continue to drive cloud adoption through IT modernization assessments, IT Strategy Plans, educating and upskilling their workforces in the areas of multi-cloud services, and modernizing application platforms.

6.2. Each BU should conduct regular evaluations of customer experience and user needs to ensure that their solutions successfully foster efficiency, accessibility, and privacy.

6.3. Each BU should review, rationalize and update agency applications to reduce the risk of large scale failures, better allocate their resources, and provide staff with adequate time to become more familiar with product management techniques.

6.3.1. Each BU should implement processes that continually evaluate and reduce IT costs, align applications with business capabilities, and reduce technology risks.

6.3.2. Each BU should invest in modernizing their application portfolios to ensure the application meets the needs of the business and its target customers.

6.4. Each BU shall evaluate all new and existing information technology investments, including but not limited to those investments for technology upgrades or modernization projects, for the selection of an appropriate choice between:

6.4.1. A cloud system

6.4.2. An agency-managed system

6.4.3. A hybrid approach utilizing both cloud and agency-managed systems

6.4.4. The use of a Commercial-Off-The-Shelf (COTS) solution that may or may not utilize any of the previous systems, or,

6.4.5. Developing a custom solution utilizing any of the previous

6.5. The BU will document their decision with key points, inputs, and arguments for selecting their choice. The preference, where available and practicable, should be to utilize a COTS cloud solution.

6.6. The platform must have one or more of the following authorizations based on the identified data classification: AZRamp, StateRAMP, or one of the three levels of FedRAMP. If the chosen platform does not have any of these authorizations, then the BU must either seek authorization prior to transmitting to or creating confidential data on the platform, or complete a Risk Acceptance Form and submit it to AZDOHS.

6.7. Considerations into the evaluation should include, but not be limited to:

6.7.1. How it will affect the agency's capabilities internally and externally, now and into the future

6.7.2. How well the solution will serve the agency's long-term goals

6.7.3. How well the solution will integrate with the agency's and other state services and data to support the agency's and the State's missions and objectives with such capabilities like application modernization

6.7.4. Use and growth of the solution against budgetary constraints

6.7.5. How it will will both protect data privacy and provide appropriate data transparency

6.7.6. How it will facilitate disaster recovery, which must include the consideration of the loss of cloud services or cloud regions.

6.7.7. How the contractual terms protect the agency, the state, and its constituents

6.8. Selection of the appropriate cloud provider shall be made in the following order of precedence:

6.8.1. Software as a Service

6.8.2. Platform as a Service

6.8.3. Infrastructure as a Service

6.8.4. Public cloud / Gov Cloud

6.8.5. Off Premises - private cloud

6.8.6. Hybrid cloud

6.8.7. On Premises - private cloud

6.9. Each BU shall perform Cloud Maturity Model (CMM) assessment bi-annually OR upon a significant change to the architecture OR vendor of the application.

6.9.1. Data location (cloud, hybrid, on-prem)

6.9.2. Hardware and virtualization infrastructure

6.9.3. Continuous Improvement and Continuous Development (CI/CD)

6.9.4. Observability including monitoring

6.9.5. Applications location (cloud, hybrid, on-prem)

6.10. Each BU shall perform Cloud Security Maturity Model (CSMM) assessment bi-annually OR upon a significant change to the architecture OR vendor of the application.

6.10.1. Level 1 - Initial: No automation

6.10.2. Level 2 - Repeatable: Establishing process

6.10.3. Level 3 - Defined: Process automation

6.10.4. Level 4 - Managed: Guard rails in place

6.10.5. Level 5 - Optimized: Full Automation

6.11. Each BU shall include the following information in their annual IT Plan submission to ADOA:

6.11.1. Use of cloud computing services

6.11.2. Current plans for the expansion of cloud computing to leverage a utility-based model

6.11.3. Any security and/or operational benefits of transitioning to cloud computing

6.11.4. Any factors delaying or inhibiting the expansion of cloud computing usage

6.11.5. Plans for addressing gaps in their compliance with this policy

7. DEFINITIONS AND ABBREVIATIONS

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

7.2. “Arizona Procurement Code'' is defined by A.R.S. § 41-2501 et. seq. and Arizona Administrative Code A.A.C. R2-7-101 et.seq.

7.3. “Cloud Computing” shall have the meaning provided by the National Institute for Standards and Technology (NIST) Special Publication 800-145 and any amendatory or superseding document thereto.

8. REFERENCES

8.1. Statewide Policy P1360 - Information Technology Planning Policy

8.2. A.R.S. § 41-2501

8.3. A.C.C R2-7-101

8.4. Cloud Maturity Model (CMM)

8.5. Cloud Security Maturity Model (CSMM)

8.6. NIST 800-145, The NIST Definition of Cloud Computing, September 2011

9. VERSION HISTORY

Date	Change	Revision	Signature
11/13/2017	<DRAFT>	Draft	Jason Simpson, State CTO
4/16/2018	Minor revisions and updates	Draft	J.R. Sloan, State CTO - Deputy State CIO
6/21/2018	Clarifications and additions to address comments.	1.0	J.R. Sloan, State CTO & Deputy State CIO Jeff Wolkove - State Data Management Architect
6/4/2019	Clarification in 6.3 regarding PIJ process and the reporting of staff augmentation costs	1.1	J.R. Sloan, State CTO & Deputy State CIO
9/6/2023	Approach to policy changed. Renamed from Cloud First Policy to Cloud Smart Policy.	2.0	J.R. Sloan, State CIO