| ARIZONA DEPARTMENT OF ADMINISTRATION | Arizona Strategic Enterprise Technology Office<br>**STATEWIDE POLICY** | State of Arizona |
|---|---|---|

# POLICY 1100: CLOUD FIRST

| | |
|---|---|
| **DOCUMENT NUMBER:** | **P1100** |
| **EFFECTIVE DATE:** | **May 1, 2018** |
| **REVISION:** | **DRAFT 1.0** |

## 1. AUTHORITY

To effectuate the mission and purposes of the Arizona Department of Administration (ADOA), ADOA shall establish a coordinated plan and program for information technology (IT) implemented and maintained through policies, standards and procedures (PSPs) as authorized by Arizona Revised Statutes (A.R.S.) § 18-104 and § 18-105. REFERENCE STATEWIDE POLICY FRAMEWORK P8280 ACCEPTABLE USE.

## 2. PURPOSE

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 (as defined below) covered by this policy in the State of Arizona (the "State"). The goal is to promote and encourage the use of cloud technologies by Budget Units.

## 3. SCOPE

**3.1** **Application to Budget Units** - This policy shall apply to all Budget Units (BUs) as defined in A.R.S. § 18-101(1).

**3.2** **Application to Systems** - This policy shall apply to all BU information systems. The content of this policy is primarily focused on server, infrastructure, and software application technologies, unless specified otherwise.

## 4. EXCEPTIONS

**4.1** If a BU needs an exception from this Policy, they must request and obtain approval from both the State Chief Information Officer (CIO) and State Chief Technology Officer (CTO). If approved, the exception is allowed for up to 24 months. At the expiration of the exception term, the BU must reassess moving to the cloud and seek a new exception from the CIO and CTO. This applies to all hardware refreshes, software applications and any other IT spending.

**4.2** Desktops/Laptops/Mobile Devices are exempted from this policy. However, BUs are encouraged to leverage thin or zero clients in combination with desktop as a service in order to reduce costs and increase security.

## 5. ROLES AND RESPONSIBILITIES

**5.1** State Chief Information Officer (CIO) shall:

**5.1.1** Subject to the requirements of the Arizona Procurement Code, 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.

**5.2** State Chief Technology Officer (CTO) shall:

**5.2.1** Subject to the requirements of the Arizona Procurement Code, be responsible for reviewing and approving vendors that provide cloud solutions, including infrastructure, platforms and software.

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

**5.3** State Chief Information Security Officer (CISO) shall:

**5.3.1** Advise the State CIO on cloud infrastructure, platforms and software that meet the State security policies.

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

**5.4** BU Director shall:

**5.4.1** Be responsible for approving a plan to migrate all information systems to the cloud by July 1, 2021.

**5.4.2** Promote efforts within the BU to establish and maintain effective use of cloud systems going forward.

**5.5** BU CIO shall:

**5.5.1** Develop a plan to migrate all information systems to the cloud by June 30, 2021.

**5.5.2** Actively migrate all infrastructure to the cloud by June 30, 2021.

**5.5.3** Ensure that the State security policies are met by the cloud vendors.

## 6. POLICY

**6.1** **Cloud Computing Services** - All BUs are required to use commercial cloud computing services and commercial cloud-based applications, for any new information technology investment. Additionally, any information technology upgrades or modernization projects must also leverage cloud computing services and/or cloud application providers. If a BU needs an exception from the foregoing requirements, it must follow the process listed in section 4.1.

**6.2** The Project Investment Justification (PIJ) process will be amended to require and support this Policy and require compliance with all applicable statewide security policies.

**6.3** The PIJ process will be amended to require any project spending more than $25,000 that includes staff augmentation be reviewed and approved by ASET.

**6.4** For the purposes of this Policy, the term "cloud computing" shall have the meaning given that term by the National Institute for Standards and Technology in NIST Special Publication 800-145 and any amendatory or superseding document thereto.

**6.5** Each BU shall provide an annual written report to the Office of the Governor and the State CIO by May 30th on the use of commercial cloud computing services, current plans for the expansion of cloud computing to leverage a utility-based model, any security benefits of transitioning to cloud computing, and any factors delaying or inhibiting the expansion of cloud computing usage.

## 7. DEFINITIONS AND ABBREVIATIONS

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

**7.2** "Arizona Procurement Code" means A.R.S. § 41-2501 et. seq. and A.A.C. R2-7-101 et.seq.

## 8. REFERENCES

**8.1** Statewide Policy Exception Procedure

**8.2** STATEWIDE POLICY FRAMEWORK 8110, Data Classification and Handling

**8.3** STATEWIDE POLICY FRAMEWORK 8120, Information Security Program Policy

**8.4** STATEWIDE POLICY FRAMEWORK 8220, System Security Maintenance

**8.5** STATEWIDE STANDARD 8220, System Security Maintenance

**8.6** STATEWIDE POLICY FRAMEWORK 8250, Media Protection

**8.7** STATEWIDE POLICY FRAMEWORK P8280 Acceptable Use

**8.8** STATEWIDE POLICY FRAMEWORK 8320, Access Control

**8.9** STATEWIDE POLICY FRAMEWORK 8340, Identification and Authentication

**8.10** STATEWIDE STANDARD 8350, System and Communication Protection

**8.11** NIST 800-53 Rev. 4, Recommended Security Controls for Federal Information Systems and Organizations, February 2013, January 2012

**8.12** NIST 800-145, The NIST Definition of Cloud Computing, September 2011

**8.13** HIPAA Administrative Simplification Regulation, Security and Privacy, CFR 45 Part 164, February 2006

**8.14** Payment Card Industry Data Security Standard (PCI DSS) v2.0, PCI Security Standards Council, October 2010.

**8.15** IRS Publication 1075, Tax Information Security Guidelines for Federal, State, and Local Agencies: Safeguards for Protecting Federal Tax Returns and Return Information, 2010.

**8.16** General Records Retention Schedule for All Public Bodies, Electronic Communications, Social Networking and Website Records, Schedule Number 000-12-22, Arizona State Library, Archives and Public Records

## 9. ATTACHMENTS

None.

## 10. REVISION 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 |