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

DRAFT P1000 - Information Technology Governance Policy

Document Number:	P1000
Effective Date:	3/24/2023
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 establish positive and effective governance over Information Technology and ensure that information technology services support the budget unit's (BUs) mission, strategy and stakeholder requirements in an efficient and effective manner.

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. Roles And Responsibilities

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

4.1.1. Be responsible for defining Statewide IT PSPs as authorized by Arizona Revised Statute A.R.S. § 18-104.

4.1.2. Be responsible for ensuring that appropriate IT Governance policies are adopted to create a responsible, safe, and resilient IT environment for the state government and its agencies to operate within.

4.2. Budget Unit Chief Information Officer (CIO) or his/her designee shall be responsible for ensuring that their BU effectively implements and adopts this policy and supporting policies to create a responsible, safe, and resilient IT environment for their BU, and their interactions or interoperability with other BUs.

4.3. 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.

4.4. Employees and contractors shall adhere to all state and BU policies, standards and procedures pertaining to the use of the State IT resources.

5. Policy

5.1. Each BU shall implement and maintain an IT governance framework consistent with the Arizona Revised Statutes and Administrative Rules and in accordance with this policy. The BU shall ensure that IT-related processes are overseen effectively and transparently in line with the BU's strategies and objectives.

5.2. Each BU, in accordance with P1360 IT Planning Policy, and in accordance with A.R.S. § 18-104 A, will develop and follow a three year IT strategic plan that is submitted to ADOA-ASET.

5.3. Each BU will develop and maintain a Disaster Recovery Plan in accordance with A.R.S. § 18-104 A.1.(f) as defined in A.R.S. § 18.101.5.

5.4. Each BU will develop and maintain Quality Assurance Plans in accordance with A.R.S. § 18-104 A.1.(f) as defined in A.R.S. § 18.101.

5.5. Each BU shall maintain Executive Level approval and ongoing visibility into IT projects, risks and the state of the BU's IT environment.

5.6. Utilizing statewide operational standards, each BU shall monitor the performance metrics, consistent with :ean principles such as those used in the Arizona Management System (AMS), to determine the extent to which the BU is generating the expected value and benefits to the BU from IT-enabled investments and services. Each BU shall also identify significant issues and develop and document corrective action plans.

5.6.1. Each BU shall collect relevant, timely, complete, credible and accurate data to report on progress in delivering value against targets. BUs shall obtain a succinct, high-level, all-around view of portfolio, program and IT performance that supports decision-making, and ensure that expected results are being achieved from initiation, through check-ins and continue on any and all implementations through project close and subsequent maintenance.

5.7. Each BU engaging in projects shall use a project management system and methodology appropriate for the projects being managed. For projects above the minimum Project Investment Justification (PIJ) threshold, each BU will follow the PIJ policies, standards and procedures in accordance with P3400 Project Investment Justification (PIJ) Policy.

5.8. Each BU shall assign a project manager and establish appropriate governance and control, communication, quality, change, and risk management plans all of which are to be developed throughout the life of the project. Projects should be effectively managed within the limitations of scope, time, budget, and risks.

5.9. Each BU shall implement and comply with statewide IT and Security PSPs, in accordance with P1050 Policy Standard and Procedure Policy and also in accordance with the Arizona Department of Homeland Security PSPs.

5.10. Applicable National and State standards should be adopted where applicable including without limitation the following: Information Technology Infrastructure Library (ITIL), National Institute of Standards and Technology (NIST) (SP 800-145 - The NIST Definition of Cloud Computing; SP 800-53 – NIST Risk Management Framework), Center for Internet Security (CIS) compliance - For Patching and Vulnerability, Data Management Capability Assessment (DCAM), Cloud Data Management Capabilities (CDMC), National Emergency Number Association (NENA), and Arizona Department of Homeland Security Policies, Standards, and Procedures.

5.11. Prior to issuing and evaluating project procurement vehicles, including requests for proposals (RFPs), the BU will document their decision with key points, inputs and

arguments for selecting appropriate solutions that align with and are in compliance with the P1100 Cloud Smart Policy and other applicable technical policies, standards and procedures.

5.12. Each BU will ensure that a Change Advisory Board (CAB) is appointed to oversee the stability and maintenance of all production environments, in accordance with P1550 Change Control & Management Policy.

6. Definitions And Abbreviations

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

7. References

7.1. A.R.S. § 18-104

7.2. A.R.S. § 18-101

7.3. P3400 Project Investment Justification (PIJ) Policy
https://aset.az.gov/policies-standards-and-procedures

7.4. Arizona Management System (AMS): “An intentional, results-driven approach for doing the work of AZ state government” See https://results.az.gov/arizonas-approach for more information.

7.5. P1360: Information Technology Planning
https://aset.az.gov/policies-standards-and-procedures

7.6. P1050: Policy Standard And Procedure Policy
https://aset.az.gov/policies-standards-and-procedures

7.7. Arizona Department of Homeland Security
https://azdohs.gov/information-security-policies-standards-and-procedures

7.8. P1100: Cloud Smart Policy
https://aset.az.gov/policies-standards-and-procedures

7.9. P1550 Change Control & Management Policy
https://aset.az.gov/policies-standards-and-procedures

7.10. Arizona Department of Homeland Security Policies, Standards, and Procedures
https://azdohs.gov/information-security-policies-standards-and-procedures

7.11. ITIL https://www.axelos.com/certifications/itil-service-management/

7.12. NIST 800-145 The NIST Definition of Cloud Computing
https://csrc.nist.gov/publications/detail/sp/800-145/final

7.13. NIST SP 800-53 Security and Privacy Controls for Information Systems and Organizations
https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final

7.14. CIS Critical Security Control 7: Continuous Vulnerability Management
https://www.cisecurity.org/controls/continuous-vulnerability-management

7.15. Data Management Capability Assessment (DCAM)
https://edmcouncil.org/frameworks/dcam/

7.16. Cloud Data Management Capabilities (CDMC)
https://edmcouncil.org/frameworks/cdmc/

7.17. National Emergency Number Association (NENA)
https://www.nena.org/

7.18.

8. VERSION HISTORY

Date	Change	Revision	Signature
3/31/2023	Major Revision	2.0	

10/11/2016	Updated all State Statutes	1.1	Morgan Reed, State CIO and Deputy Director
9/01/2014	Initial Release	1.0	Arun Sandeen, State CIO and Deputy Director