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

P6100: STATE SHARED HOSTED DATA CENTER (SHDC) INFRASTRUCTURE CONFIGURATION MANAGEMENT AND CHANGE CONTROL

DOCUMENT NUMBER:	**P6100**
EFFECTIVE DATE:	**JULY 2, 2021**
REVISION NUMBER:	**1.2**

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. 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.

2. PURPOSE

The purpose of this policy is to establish the baseline controls for management and maintenance of state information systems. [National Institute of Standards and Technology (NIST) 800-128] [NIST 800-53 CM1-CM9]

3. SCOPE

3.1 This policy applies to all Divisions of ADOA and IT integrations and/or data exchange with third parties that perform functions, activities or services for or on behalf of the Agency or its Divisions through the State Shared Hosted Data Center (SDC). Applicability of this policy to third parties is governed by contractual agreements entered into between ADOA and the third party/parties.

3.1.1 Application to Systems - This policy shall apply to all state information systems. Categorization of systems is defined within Policy 8120, Information Security Program.

3.2 Application to Third Parties - This Policy shall apply to all ADOA vendors and contractors providing goods and services to the ADOA and to third parties, including other Government bodies.

4. ROLES AND RESPONSIBILITIES

Note: The types of roles defined are accountable for the SHDC acceptance and adherence to the SHDC Configuration Management and Change Control. For a conclusive list of roles and responsibilities regarding Configuration Management and Change Control will be defined within the process documents.

4.1 State Chief Information Officer (CIO) shall:

a. Be ultimately responsible for the correct and thorough completion of Statewide IT PSPs throughout all state BUs.

4.2 Chief Operating Officer (COO), Cloud Ops Director, Sate Shared Hosted Data Center Manager shall:

a. Oversee the management and operation of the State Shared Hosted DataCenter;

b. Make decisions, with respect to, the application of State policies and Arizona Revised Statutes to the SHDC;

c. Be the ultimate authority to ensure that contracted service delivery and support commitments are met, including but not limited to, making decisions regarding spending levels, acceptable risk, and interagency coordination of service events and decisions requiring their concurrence; and

d. Lead the SHDC management team in its accomplishment of specific responsibilities critical to the delivery and support of SHDC services.

4.3 ADOA-ASET Change Manager shall:

NOTE: The Change Manager is responsible for the coordination of the Change Management process and the management of the policies, procedures and tools that support the process to ensure compliance for all system changes.

a. Ensure Change Management procedures are adhered to by all parties;

b. Ensure that participants in the Change Management process are properly trained;

c. Provide change management reports to management for review and evaluation;

d. Chairs the Change Advisory Board (CAB) meetings;

e. Oversight and approval of Emergency Changes;

f. Issue and publish Change Schedules;

g. Based on the complexity of the change, ensures that a Post Implementation Review was performed on implemented changes;

h. Ensure that the business or technical impact of the change is clearly communicated;

i. Ensure that content of the Change Request is complete, detailed, and sufficiently documents all components of the proposed change, the reason for the change and the work effort; and

j. Approve, challenge or reject Change Requests submitted for implementation.

4.4 Change Implementers shall:

Note: Change Implementers are the individuals conducting the requested change;

a. Ensure that appropriate approvals are obtained prior to starting activities related to the requested change;

b. Keep the status of the Change Request current by updating the Change Request record or by communication with the Requestor; and

c. Adherence to the approved change schedule.

4.5 Change Advisory Board shall: [NIST 800 53 CM-3] [IRS Pub 1075]

a. Determine the types of changes to the information system that are configuration-controlled;

b. Review proposed configuration-controlled changes to the information system and approves or disapproves such changes with explicit consideration for security impact analysis;

c. Document configuration changes and decisions associated with the information system;

d. Implement approved configuration-controlled changes to the information system; and retain activities associated with configuration-controlled changes to the information system.

5. POLICY

The principal objective of the Configuration Management and Change Control is to document production system baselines and manage changes in a rational and predictable manner so that staff and clients can plan accordingly. This in turn will aid the SDC to recover mission critical and essential systems from an unforeseen event, disaster or emergency that interrupts information systems and business operations, as quickly and effectively as possible.

6. DEFINITIONS AND ABBREVIATIONS

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

7. REFERENCES

7.1 A.R.S. § 18-104, § 18-107

7.2 Statewide Policy Framework P1050 - IT POLICIES, STANDARDS & PROCEDURES PROGRAM

7.3 ADOA Policy 8120, Information Security Program

7.4 NIST Special Publication 800-53 Rev. 4. Recommended Security Controls for Federal Information Systems andOrganizations

7.5 NIST Special Publication 800-128 Guide for Security-Focused Configuration Management of Information Systems

7.6 FBI Criminal Justice Information Services (CJIS) Security Policy Version 5.9 06/01/2020

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

8. ATTACHMENTS

None.

9. Revision History

Date	Change	Revision	Signature0
9/01/2014	Initial Release	Draft	Aaron Sandeen, State CIO and Deputy Director
10/11/2016	Updated all the Security Statutes	1.0	Morgan Reed, State CIO and Deputy Director
11/26/2018	Annual update	1.1	Morgan Reed, State CIO and Deputy Director
6/21/2021	Copied into new format and reviewed for annual updates, added IRS Pub 1075 and FBI Criminal Justice Information Services (CJIS) references.	1.2	Randy Wheaton
7/2/2021	Approved		J.R. Sloan, State CIO