1. **AUTHORITY**

To effectuate the mission and purposes of the Arizona Department of Administration (ADOA), the Agency 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 § 18-107.

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 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. **EXCEPTIONS**
The Exception process allows Assistant Directors to make an informed decision on whether or not to request an exception to a particular SDC policy by understanding the risk and alternatives involved.

5. ROLES AND RESPONSIBILITIES

Note: The types of roles defined are accountable for the SDC acceptance and adherence to the SDC 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.

5.1 State Chief Information Officer (CIO) shall:
   a. Be ultimately responsible for the correct and thorough completion of Statewide IT PSPs throughout all state BUs.

5.2 Chief Operating Officer (COO), Assistant Director, State Data Center Manager shall:
   a. Oversee the management and operation of the State Data Center;
   b. Make decisions, with respect to, the application of State policies and Arizona Revised Statutes to the SDC;
   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 SDC management team in its accomplishment of specific responsibilities critical to the delivery and support of SDC services.

5.3 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;

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.

5.4 Change Implementer 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.

5.5 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 change decisions associated with the information system;

d. Implement approved configuration-controlled changes to the information system; and

e. Retain activities associated with configuration-controlled changes to the information system.

6. 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.

### 6.1 System Configuration Management [NIST 800 53 CM-9]

#### 6.1.1 Configuration Management Plan - SDC shall develop, document, and implement a configuration management plan for information systems that will:

- Address the roles, responsibilities, and configuration management processes and procedures;
- Establish a process for identifying and managing configuration items;
- Define the configuration items for the information systems, regardless of residency, whether in the SDC or at a remote or virtual location and place the configuration items under configuration change management control; and
- Protect the configuration management plan from unauthorized disclosure and modification.

#### 6.1.2 Baseline Configuration - SDC shall develop, document, and maintain a current baseline configuration for information systems managed or owned. [NIST 800 53 CM-2] [IRS Pub 1075]

- **Baseline Configuration Reviews and Updates** - SDC shall review and update the baseline configurations for information systems, at least annually, upon significant changes to system functions or architecture, and as an integral part of system installations and upgrades. [NIST 800-53 CM-2 (1)] [IRS Pub 1075];

#### 6.1.3 Inventory Reviews and Updates - SDC shall review and update the information system component inventory periodically, at minimum annually, and as an integral part of component installations, removals, and information system updates. [NIST 800 52 CM-8 (1)];

#### 6.1.4 Detection of Unauthorized Hardware, Software, and Firmware Components – The SDC shall employ:

- **Automated mechanisms to detect the presence of unauthorized hardware, software, and firmware components within the information system and take appropriate actions to disable network access, isolate the component, or notify the appropriate personnel of the unauthorized component.** [NIST 800 53 CM-8 (3)] [IRS Pub 1075].

- **If automated mechanisms are not in place, the SDC shall employ adequate compensating controls that prevent the introduction of unauthorized hardware, software, and firmware components.**
6.2 **Configuration Change Control** - SDC shall establish and maintain a Change Advisory Board in order to:

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

b. Approve configuration-controlled changes to the system with explicit consideration for impact analyses;

c. Document approved configuration-controlled changes to the system;

d. Retain and review records of configuration-controlled changes to the system;

e. Audit activities associated with configuration-controlled changes to the system.

f. Ensure communication of all changes and potential impact to stakeholders.

7. **Definitions and Abbreviations**

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

8. **References**

8.1 A.R.S. § 18-104, § 18-107

8.2 ADOA Policy P100, Information Technology

8.3 ADOA Policy 8120, Information Security Program

8.4 NIST Special Publication 800-53 Rev. 4. Recommended Security Controls for Federal Information Systems and Organizations

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

9. ATTACHMENTS

None.

10. REVISION HISTORY

<table>
<thead>
<tr>
<th>Date</th>
<th>Change</th>
<th>Revision</th>
<th>Signature</th>
</tr>
</thead>
<tbody>
<tr>
<td>07/10/2014</td>
<td>Initial Release</td>
<td>1.0</td>
<td>Aaron Sandeen, State CIO and Deputy Director</td>
</tr>
<tr>
<td>10/11/2016</td>
<td>Updated all the Security Statutes</td>
<td>1.0</td>
<td>Morgan Reed, State CIO and Deputy Director</td>
</tr>
</tbody>
</table>