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

DRAFT P1550 - CHANGE CONTROL & MANAGEMENT POLICY

DOCUMENT NUMBER:	P1550
EFFECTIVE DATE:	10/31/2022
VERSION:	1.0

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 document is to describe the process by which ADOA/ASET manages changes to production information systems and technologies. The underlying purpose is to maximize systems, operations and data availability within the State Data Center (SDC) and to ensure that changes are managed to minimize disruption to business operations. The change control process ensures the consistent and effective process of planning, scheduling, communicating and implementing changes successfully.

3. SCOPE

3.1. 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 (BUs). 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 ensuring that a Change Advisory Board (CAB) is appointed to oversee the stability and maintenance of the production environment for which the State CIO is responsible.

4.2. Budget Unit Chief Information Officer (CIO) or his/her designee shall:

4.2.1. Be responsible for ensuring that a Change Advisory Board (CAB) is appointed to oversee the stability and maintenance of the production environment for which the Budget Unit CIO is responsible.

4.3. Individual BU Users shall:

4.3.1. Become familiar with statewide and agency specific IT PSPs.

4.3.2. Adhere to statewide and agency specific IT PSPs pertaining to the use of State and/or BU IT resources.

5. POLICY

5.1. Each BU shall establish a Change Advisory Board (CAB).

5.1.1. The CAB shall be composed of representatives of IT teams responsible for reviewing normal change requests. (Change Owners / Assignees / Implementers also attend CAB meetings to represent their changes.)

5.1.2. The CAB reports to the Chief Operating Officer of the BU or a similar role designated by the BU Chief Information Officer.

5.1.3. The CAB shall be responsible for review of normal change requests and shall establish and publish procedures for submitting proposed changes.

5.1.4. The CAB shall meet regularly to review pending change requests.

5.2. All proposed changes must be approved by the CAB following the published procedure.

5.2.1. All changes to production configuration items (CIs) require the completion and submission of a Change Request (CR). The Change Advisory Board (CAB) must approve the change prior to deployment.

5.3. The CAB shall maintain a change calendar, including a change blackout calendar.

5.4. Change Types:

5.4.1. Normal changes are required to be reviewed at the CAB meeting for CAB approval. Normal changes are pre-planned and scheduled such that they can be implemented within the normal approval cycle and implementation windows.

5.4.2. Emergency changes must be related to active Priority 1 or 2 Incidents (see Section 6. Definitions and Abbreviation). Emergency changes are commonly referred to as emergency break fix items. The main concern is to fix the issue and get users productive again. The majority of Emergency changes are time sensitive and do not have the leeway to take the time to go through the process for CAB approval. Emergency change tickets are required for the change; however, due to the nature of their use, one business day is allowed to complete documentation of the change. (May also be related to problems and if caused by a previous change, subject to post-implementation reviews) These changes do not go through the CAB but do require approval by the Change Manager and may require CIO and/or senior level management approval (Senior Management in the reporting structure of the change) depending on their complexity and impact. Emergency changes must be reviewed by CAB post-implementation.

5.4.3. Standard changes are common, pre-approved maintenance items, utilizing templates in the ticketing system. There are no ad hoc standard changes. These changes do not go through the CAB as they are routine in nature and pose a low risk to the availability of services provided to the business. Standard changes are approved by the Manager of the Change Assignee / Implementer.

5.5. Risk Assessment

5.5.1. In order to provide consistency in how changes are categorized for review and approval, a risk assessment must be done for all production change tickets. Several factors must be taken into consideration for the risk level of a change. These factors include:

5.5.1.1. Impact – How does this change impact the business, does it impact production and will it require an outage during business hours?

5.5.1.2. Affected areas – Is the entire organization affected or a single site or workgroup?

5.5.1.3. Complexity – How complex is the change – does it require technical and business coordination, as in require coordination among technical teams, or is it a routine maintenance change that has been done successfully in the past?

5.6. Failure to comply with the Change Control & Management Policy may result in disciplinary actions, up to and including termination.

6. Definitions And Abbreviations

Refer to the Policies, Standards and Procedures Glossary located on the ADOA-ASET website.

Priority 1 Incident: A core business IT service is unavailable and must be restored immediately to minimize a direct financial, brand, or security impact on the business organization.

Priority 2 Incident: An IT service is unavailable or degraded, impacting a large group of users, and must be restored within 4 hours to minimize a direct financial, brand, or security impact on the business organization.

7. References

7.1. A.R.S. § 18-101

7.2. A.R.S. § 18-104

7.3. Standard S1550: Change Control & Management Standard

7.4. Procedure PR1550: Change Control & Management Procedure

8. Links

9. Version History

Date	Change	Revision	Signature
10/31/2022	Initial Version	1.0	