

<p>ARIZONA DEPARTMENT OF ADMINISTRATION</p>	<p>Arizona Strategic Enterprise Technology Office STATEWIDE POLICY</p>	 <p>State of Arizona</p>
--	---	--

P1650: RELEASE MANAGEMENT POLICY

DOCUMENT NUMBER:	P1650
EFFECTIVE DATE:	OCTOBER 11, 2016
REVISION:	1.1

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.

2. PURPOSE

The purpose of this policy is to ensure that application software solutions and services are implemented safely and consistent with agreed upon expectations and outcomes.

3. SCOPE

- 3.1** Application to Budget Units (BUs) - This policy shall apply to all BUs and IT integrations and/or data exchange with third parties that perform functions, activities or services for or on behalf of the BU as defined in A.R.S. § 18-101(1).
- 3.2** Application to Third Parties - This Policy shall apply to all State of Arizona vendors and contractors providing goods and services to the State and to third parties, including other government bodies. Applicability of this policy to third parties is governed by contractual agreements entered into between the BU and the third party.

4. EXCEPTIONS

- 4.1** PSPs may be expanded or exceptions may be taken by following the Statewide Policy Exception Procedure.
 - 4.1.1** In the case of existing IT Products and Services, BU subject matter experts (SMEs) should inquire with the vendor and the state or agency procurement office to ascertain if the contract provides for additional products or services to attain compliance with PSPs prior to submitting a request for an exception in accordance with the Statewide Policy Exception Procedure.

- 4.1.2** Prior to selecting and procuring information technology products and services, BU SMEs shall comply with Statewide IT PSPs when specifying, scoping, and evaluating solutions to meet current and planned requirements.

5. ROLES AND RESPONSIBILITIES

- 5.1** State Chief Information Officer (CIO) shall be ultimately responsible for the correct and thorough completion of Statewide IT PSPs throughout all state BUs.
- 5.2** BU Chief Technology Officer (CTO) or a person delegated these responsibilities shall:
 - 5.2.1** Be responsible for all application software selection and implementation by the BU;
 - 5.2.2** Review and approve all application software projects prior to release to production;
 - 5.2.3** Monitor all application software projects after release; and
 - 5.2.4** Ensure that all new application software complies with this policy.
- 5.3** Program Manager or a person delegated these responsibilities shall:
 - 5.3.1** Develop the implementation plan for all new application software and services;
 - 5.3.2** Ensure that the plan has been reviewed and approved prior to promoting the service to production; and
 - 5.3.3** Implement the plan as approved.
- 5.4** The Quality Assurance Manager or a person delegated these responsibilities shall:
 - 5.4.1** Ensure that QA testing is performed to plan; and
 - 5.4.2** Ensure that all errors are remediated and retested prior to promotion.

6. STATEWIDE POLICY

- 6.1** BUs shall develop and document a test plan that defines roles, responsibilities, and entry and exit criteria. The responsible parties shall review and approve the plan prior to data conversion and system modifications.
 - 6.1.1** The test plan shall include the following components, as appropriate:
 - a. Unit test;
 - b. System test;
 - c. Integration test;

- d. User acceptance test (UAT);
- e. Performance test;
- f. Stress test;
- g. Data conversion test;
- h. Operational readiness test; and
- i. Backup and recovery tests.

6.1.2 BUs shall establish a test environment representative of planned business process and IT operations using representative data that has been scrubbed to obfuscate private information. If confidential information is used in the test environment, it is required to be protected at the same level that it is protected in the production environment in accordance with applicable statewide Information Security Policies.

6.2 BUs shall perform acceptance testing as appropriate and consistent with the implementation plan.

6.2.1 Designated persons shall review error logs and develop and implement remediation including additional testing to verify that the errors have been effectively addressed.

6.2.2 Designated persons shall communicate the results of acceptance testing to designated stakeholders for their review and comment.

6.2.3 Designated persons shall ensure final acceptance by business process owners and stakeholders prior to promotion to the production environment.

6.3 BUs shall develop and document an implementation plan for all new application software and services covering:

- a. System and data conversion, if applicable;
- b. Acceptance testing criteria;
- c. Communication;
- d. Training;
- e. Release preparation;
- f. Promotion to production;
- g. Production support;
- h. A fallback or back-out plan; and
- i. A post-implementation review

- 6.3.1** The implementation plan shall reflect the implementation strategy, sequence of steps, resource requirements, inter-dependencies, criteria for management acceptance, installation verification requirements, transition strategy for production support, and update of the business continuity plan (BCP).
 - 6.3.2** The implementation plan shall be reviewed and approved by technical and business process stakeholders prior to promotion to production.
 - 6.3.3** BU management shall review the technical and business risk associated with implementation and ensure that all significant risks are identified and mitigated prior to implementation.
- 6.4** BUs shall develop and document a business process, system and data conversion plan encompassing all changes including:
- a. Hardware;
 - b. Networks;
 - c. Operating systems;
 - d. Transaction data;
 - e. Master files;
 - f. Backups and archives;
 - g. Interfaces with other systems;
 - h. Compliance requirements;
 - i. Business procedures; and
 - j. System documentation.
- 6.4.1** BUs shall test the conversion before attempting to convert live data.
 - 6.4.2** BUs shall ensure that a fallback plan is developed and adequate preparation is made, including necessary backups, prior to conversion of data.
- 6.5** BUs shall promote new application software and services to the production environment using change controls and management and monitor the results after the change has been communicated to process owners and stakeholders.
- 6.6** BUs shall provide support to users after promotion to production.
- 6.7** BUs shall conduct and document a post-implementation review to confirm the outcome and results.

7. DEFINITIONS AND ABBREVIATIONS

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

8. REFERENCES

Arizona Revised Statutes § 18-104

<http://csrc.nist.gov/publications/nistpubs/800-122/sp800-122.pdf>

9. ATTACHMENTS

(none)

10. REVISION HISTORY

Date	Change	Revision	Signature
10/11/2016	Updated all the Security Statutes	1.0	Morgan Reed, State CIO and Deputy Director