

CHAPTER: 100

Agency Administration/Management

DEPARTMENT ORDER:

126 – Vendor Management

OFFICE OF PRIMARY  
RESPONSIBILITY:

FS

Effective Date:

August 30, 2024

Amendment:

N/A

Supersedes:

DO 126 (2/10/21)

Scheduled Review Date:

2027

ACCESS

**Contains Restricted Section(s)**

# Arizona Department of Corrections Rehabilitation and Reentry



Department Order Manual

A handwritten signature in black ink, appearing to read "Ryan Thornell", is written over a horizontal line.

Ryan Thornell, Director

## TABLE OF CONTENTS

<b>PURPOSE .....</b>	<b>1</b>
<b>APPLICABILITY .....</b>	<b>1</b>
<b>PROCEDURES .....</b>	<b>1</b>
<b>1.0 GENERAL RESPONSIBILITIES .....</b>	<b>1</b>
<b>2.0 THIRD PARTY VENDOR AGREEMENTS .....</b>	<b>2</b>
<b>3.0 PROGRAM MANAGEMENT .....</b>	<b>3</b>
<b>DEFINITIONS/GLOSSARY .....</b>	<b>5</b>
<b>AUTHORITY .....</b>	<b>6</b>

## **PURPOSE**

This Department Order (DO) establishes standards to effectively manage Information Technology vendor contracts to assure the best possible outcome for the state and Department.

## **APPLICABILITY**

This DO applies to all Information Technology contracts with third-party providers that have a critical impact on the success of strategic projects and services and;

- Have an expected duration of twelve or more months;
- Carry significant risk to the Department or its stakeholders;
- Play a vital role in operations;
- May require continuous monitoring;
- Have complex dispute and problem-solving mechanisms;
- Or access or manage substantial critical, sensitive, or confidential data.

## **PROCEDURES**

### **1.0 GENERAL RESPONSIBILITIES**

#### 1.1 The Director shall:

- 1.1.1 Be responsible for the correct and thorough completion of Department Policies, Standards, and Procedures (PSPs).
- 1.1.2 Ensure compliance with Department PSPs.
- 1.1.3 Promote efforts within the Department to establish and maintain effective use of Department information systems and assets.

#### 1.2 The Chief Information Officer shall:

- 1.2.1 Work with the Director to ensure the correct and thorough completion of Department Information Technology PSPs.
- 1.2.2 Ensure PSPs are periodically reviewed and updated to reflect changes in requirements.

#### 1.3 The Information Security Officer shall:

- 1.3.1 Advise the Chief Information Officer on the completeness and adequacy of the Department activities and documentation provided to ensure compliance with Department and State Information Technology PSPs.
- 1.3.2 Ensure the development and implementation of adequate controls, enforcing the System Security Acquisition Policy for the Department.

- 1.3.3 Ensure all personnel understand their responsibilities with respect to secure acquisition of Department information systems and components.
- 1.4 The Chief Procurement Officer shall:
  - 1.4.1 Provide advice and support with the procurement of goods and services in regards to requests for information, requests for proposal, evaluation of response, and contract awards.
  - 1.4.2 Ensure compliance with Arizona procurement statutes and PSPs throughout the procurement process. (See DO #302, Contracts and Procurement).
- 1.5 The Business Process Owner(s) shall:
  - 1.5.1 Be responsible for the development of requirements; including the security controls specified in the Arizona Department of Administration (ADOA)/Arizona Strategic Enterprise Technology (ASET) Office Policy (P8130) System Security Acquisition and Development or equivalent Department policy.
  - 1.5.2 Support vendor selection and contract negotiation.
  - 1.5.3 Ensure the vendor agreement is conducted per the contract.
  - 1.5.4 Ensure that contract termination and transition is performed effectively and efficiently.
- 1.6 The Vendor Manager shall:
  - 1.6.1 Ensure that stakeholder requirements are complete and accurate as documented.
  - 1.6.2 Ensure that vendor responses to the Department address all requirements.
  - 1.6.3 Support vendor selection and contract negotiation.
  - 1.6.4 Establish service level agreement standards and monitor performance against these.
  - 1.6.5 Ensure that risks are identified and monitored.
  - 1.6.6 Ensure that problems, issues, disputes, and other matters are resolved timely.
  - 1.6.7 Timely communicate the status of the contract and any changes to stakeholders.
  - 1.6.8 Manage the termination and transition process.

## **2.0 THIRD PARTY VENDOR AGREEMENTS**

- 2.1 The Department shall develop PSPs for all business processes supported by third-party vendor agreements.
  - 2.1.1 PSPs shall support and supplement State Procurement Office, security and privacy, project management, and other Information Technology PSPs and guidelines.
- 2.2 Contracts shall reference all applicable PSPs and vendors shall be required to comply with each referenced PSP.

### 3.0 PROGRAM MANAGEMENT

- 3.1 The Department shall appoint and provide operational support for a Vendor Management Council or similar body that substantially assumes the responsibilities designated herein. The Vendor Management Council shall include Vendor Managers and technical and business stakeholders. If the Department has a Program Management function, then Program Managers shall be represented on the Vendor Management Council.
- 3.2 The Vendor Management Council shall:
  - 3.2.1 Develop and publish standard Vendor Management documents and templates.
  - 3.2.2 Monitor key performance metrics, performance to service level agreements, and commit resources to addressing key issues, problems, disputes, or recommended changes.
  - 3.2.3 Develop, document, and implement a process to calculate and assess penalties or rewards based on the contract terms and the vendor's performance against service level agreements.
  - 3.2.4 Participate in drafting Requests for Proposals (RFPs) to ensure they accurately reflect Department vendor management principles, standards, and expectations.
  - 3.2.5 Designate a Vendor Manager for each engagement to manage vendor activities and performance.
    - 3.2.5.1 The Vendor Manager shall report to the Vendor Management Council.
  - 3.2.6 Identify, document, and communicate, in coordination with the Business Process owner and Vendor Manger, all stakeholder requirements to be incorporated into the Statements of Work and RFP.
    - 3.2.6.1 RFPs shall include all documented requirements, expectations, service level agreements, and work products to be produced by the vendor. Measurable deliverables and service levels consistent with leading practices shall be preferred.
    - 3.2.6.2 RFPs shall include the specific procedures for adjusting the vendor deliverables to accommodate new or modified requirements.
    - 3.2.6.3 All identified stakeholders shall be invited to participate in the development and approval of requirements prior to tender of RFP and statements of work.
      - 3.2.6.3.1 Requirement changes shall be documented and communicated to all stakeholders through the proper solicitation or Contract amendment.
      - 3.2.6.3.2 Stakeholder requirements shall include key performance indicators and minimum service levels.
      - 3.2.6.3.3 Emergency and disaster recovery requirements shall be included as appropriate.

3.2.6.3.4 Risk management and compliance requirements shall be included in all RFPs and contracts as appropriate.

3.2.6.3.5 If appropriate, requirements may include third-party verification of service providers' controls and capabilities.

3.3 The Vendor Manager assigned by the Vendor Management Council shall provide the following functions:

3.3.1 Communicate program status to stakeholders consisting of vendor key performance indicators and performance service level agreements.

3.3.2 Communicate to the Chief Procurement Officer or designee the need to calculate penalties or rewards to be assessed on the vendor based on the vendor's performance against service level agreements.

3.3.3 Measure stakeholder's satisfaction in vendor performance at least annually, report the results to the Vendor Management Council annually, and implement remediation as appropriate.

3.3.4 Develop, document, and implement:

3.3.4.1 In coordination with the Vendor Management Council, a vendor communication plan featuring appropriate points of contact, backup, and escalation of routine matters, issues and problems between the vendor and the relevant Department stakeholders. The communication plan shall ensure that the Vendor Manager is copied on all communications between the vendor and the stakeholders.

3.3.4.2 A problem, issue, and dispute resolution procedure, which shall include escalation and emergency procedures.

3.3.4.3 A termination and transition plan in coordination with the Vendor Management Council, State Procurement Office, Business Process Owner, stakeholders, and the vendor.

3.3.5 Develop, document, and implement or ensure compliance with existing:

3.3.5.1 Change management procedures. These procedures shall provide for the approval, communication, timing, testing, and implementation of changes.

3.3.5.2 Compliance management procedures. These procedures shall include processes to verify the vendor complies with all policies, standards and procedures, statutes, and other appropriate industry standards. These processes may include access to third-party audits if appropriate.

3.3.5.3 Asset disposal plans including computer hardware, software, and data that complies with all security, privacy, public records retention, and data governance policies.

- 3.3.6 Develop and update annually a program risk assessment. Based on the results, the Vendor Manager shall develop, document, and implement a risk management program designed to mitigate the most critical areas of risk. The Vendor Manager shall implement continuous monitoring and report the results to the Vendor Management Council.
- 3.4 The Vendor Manager shall require the vendor of the Department information system, system component, or information system service to:
  - 3.4.1 Perform configuration management during system, component, or service (development, implementation, and operation)
  - 3.4.2 Document, manage, and control the integrity of changes to configuration items under configuration management.
  - 3.4.3 Implement only Department approved changes to the Department information systems.
  - 3.4.4 Document approved changes to the system, component, or service and the potential security impacts of such changes.
  - 3.4.5 Track security flaws and flaw resolution within the system, component, or service.
- 3.5 The Vendor Manager shall require the developer of the Department information system, system component, or information system service to:
  - 3.5.1 Create and implement a security assessment plan that provides for security testing and evaluation, at the depth of security-related functional, properties, including:
    - 3.5.1.1 Security-related externally visible interfaces
    - 3.5.1.2 High-level design
  - 3.5.2 Perform integration and regression testing for components and services and unit, integration, and system testing for systems.
  - 3.5.3 Produce evidence of the execution of the security assessment plan and the results of the security testing/evaluation.
  - 3.5.4 Implement a verifiable flaw remediation process.
  - 3.5.5 Correct flaws identified during security testing/evaluation.
  - 3.5.6 Perform threat and vulnerabilities analyses, and subsequent testing/evaluation of the as-built system, component, or service.

## **DEFINITIONS/GLOSSARY**

Refer to the Glossary of Terms for the following:

- Arizona Strategic Enterprise Technology (ASET) Office
- Computer Hardware
- Confidential Data
- Information Technology

- Sensitive/Personal/Confidential Information
- Software

## **AUTHORITY**

A.A.C. R2-15-305, Lost, Stolen, or Destroyed Nonexpendable Materials (Capital Assets)

Arizona Department of Administration Statewide Policy Framework P8130 System Security Acquisition and Development

Arizona Department of Administration Surplus Property Management Office Disposal of Information Technology Assets Directive Revision: 1.1, May 2010

Arizona Department of Administration/Arizona Strategic Enterprise Technology (ASET) 8130: System Security Acquisition and Development