TECHNICAL BULLETIN No. 009

TITLE: **Cybersecurity Risk Assessment and Management Process**

REVISION: **2 (Replaces Copier/Multi-Functional Device Security)**

DATE: **December 15, 2023**

I. Authority

A. Applicable Statute

A.R.S. § 18-101	Definitions
A.R.S. § 18-104	Powers and duties of the department; violation; classification
A.R.S. § 18-552	Notification of security system breaches; requirements; enforcement; confidentiality; civil penalty; preemption; exceptions
A.R.S. § 41-2561	Definitions
A.R.S. § 41-2562	Duties of the Director
A.R.S. § 41-4282	Statewide information security and privacy office; duties; suspension of budget unit's information infrastructure

B. Applicable Administrative Code

A.A.C. R2-7-401	Preparation of Specifications
A.A.C. R2-7-B301, *et seq.*	
A.A.C. R2-7-C301, *et seq.*	

II. Definitions

A. "Contract" means all types of state agreements, regardless of what they may be called, for the procurement of materials, services, construction, construction services or the disposal of materials. A.R.S. § 41-2503(7).

B. "Data" means documented information, regardless of form or characteristic. A.R.S. § 41-2503(10).

C. "Information Technology" means all computerized and auxiliary automated information processing, telecommunications and related technology, including

hardware, software, vendor support and related services, equipment and projects. A.R.S. § 18-101(6).

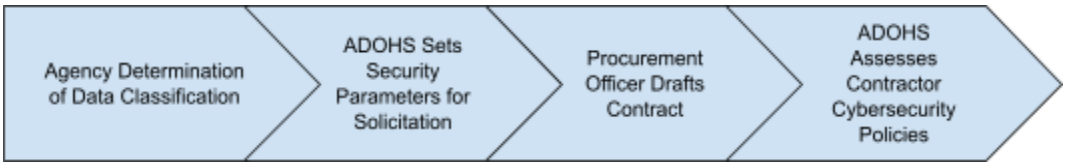
D. "Offer" means a response to a solicitation. A.A.C. R2-7-101(34).

E. "Offeror" means a person who responds to a solicitation. A.A.C. R2-7-101(35).

F. "Prospective Offeror" means a person that expresses an interest in a specific solicitation. A.A.C. R2-7-101(41).

G. "Solicitation" means an invitation for bids, a request for technical offers, a request for proposals, a request for quotations, or any other invitation or request issued by the purchasing agency to invite a person to submit an offer. A.A.C. R2-7-101(46).

III. Process



IV. Policy

A. This TB 009 formally integrates all Arizona Department of Homeland Security (ADOHS) Information Security Policies, Standards, and Procurements (at the time of the drafting of this policy available here, though this link is subject to change at any time and should be verified on the ADOHS website including, but not limited to, Data Classification policy P8110 into the Arizona Department of Administration, State Procurement Office, policies and procedures.

1. The Data Classification policy P8110 requires agencies to be responsible for securing agency information systems, including the classification and handling of Data.

2. The policy also determines what types of Data are considered confidential, and which types of Data require heightened security, like end-to-end encryption, as defined in P8110.

B. **When required by ADOHS**, agency personnel shall require use of the Arizona Risk and Authorization Management Program (AZRAMP or Program) as part of solicitation and/or contractual obligations. AZRAMP is modeled after the Federal Risk and Authorization Management Program. The following description of this Program is provided below, for convenience only, and **may be subject to change as reflected on the ADOHS website**.

1. AZRAMP is a NIST-based assessment developed to analyze a vendor's threshold for security and Data protection. Vendors must be periodically reviewed to ensure continued compliance with NIST regulation requirements.

2. The State of Arizona also recognizes StateRAMP and FedRAMP Authorizations, and may review these certifications as part of the AZRAMP process. Their authorized product list pages can be found here: https://stateramp.org/product-list/ (StateRAMP) and https://marketplace.fedramp.gov/products (FedRAMP).

3. ADOHS reserves the right to calibrate the level of security and Data protection required for any given Contract or Solicitation. A Prospective Offeror's ability to either submit an Offer on a Solicitation or be considered susceptible for a contract award under the Arizona Procurement Code may be contingent on ADOHS review of that Offeror's cybersecurity infrastructure.

C. Each State Government unit shall ensure all currently existing and future equipment purchases, rentals and leases adhere to this standard, or exceed this standard if additional security requirements are necessary based upon the business operations.

D. Agencies are responsible for Data security at every stage in the solicitation and contracting process, from ensuring appropriate requirements are in the solicitation or contract to proper disposal or transition of Data at contract termination.

E. Disposal of Data: Each State Governmental unit shall coordinate with the Surplus Property Management Office of the Arizona Department of Administration for the proper and secure disposal of physical storage media that contains or has contained state Data. Agencies shall also comply with the Statewide Standard 8250 Media Protection at: https://azdohs.gov/file/4331.

IV. Effective

This Technical Bulletin is hereby authorized and effective
this 15th day of December, 2023, unless otherwise revised or repealed.

ED Jimenez (Dec 15, 2023 15:19 MST)

Ed Jimenez
State Procurement Administrator