	STATEWIDE **POLICY**	**State of Arizona**

STATEWIDE POLICY (8230): CONTINGENCY PLANNING

DOCUMENT NUMBER:	**P8230**
EFFECTIVE DATE:	**JANUARY 30, 2025**
REVISION:	**5.0**

1. AUTHORITY

To effectuate the mission and purposes of the Arizona Department of Homeland Security, the Agency shall establish a coordinated plan and program for information security and privacy protections implemented and maintained through policies, standards and procedures (PSPs) as authorized by Arizona Revised Statutes (ARS) § 41-4254 and § 41-4282.

2. PURPOSE

The purpose of this policy is to minimize the risk of system and service unavailability due to a variety of disruptions by providing effective and efficient solutions to enhance system availability. [NIST 800-34]

3. SCOPE

3.1 Application to Budget Units (BUs) - This policy shall apply to all BUs as defined in A.R.S. § 18-101(1).

3.2 Application to Systems - This policy shall apply to all agency systems:

- **a. (P)** Policy statements preceded by "(P)" are required for agency systems categorized as Protected.
- **b.** Information owned or under the control of the United States Government shall comply with the Federal classification authority and Federal protection requirements.

4. EXCEPTIONS

4.1 PSPs may be expanded or exceptions may be taken by following the Statewide Policy Exception Procedure.

4.1.1 Existing IT Products and Services

a. 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 IT Products and Services Procurement

a. Prior to selecting and procuring information technology products and services, BU SMEs shall consider statewide information security PSPs when specifying, scoping, and evaluating solutions to meet current and planned requirements.

4.2 BU has taken the following exceptions to the Statewide Policy Framework:

Section Number	Exception	Explanation / Basis

5. ROLES AND RESPONSIBILITIES

5.1 Arizona Department of Homeland Security Director shall:

a. Be ultimately responsible for the correct and thorough completion of statewide information security PSPs throughout all State BUs.

5.2 State Chief Information Security Officer (CISO) shall:

a. Advise the Director on the completeness and adequacy of all state BU activities and documentation provided to ensure compliance with statewide information security PSPs throughout all state BUs;

b. Review and approve BU security and privacy PSPs and requested exceptions from the statewide security and privacy PSPs; and

c. Identify and convey to the Director the risk to State systems and data based on current implementation of security controls and mitigation options to improve security.

5.3 Enterprise Security Program Advisory Council (ESPAC)

a. Advise the State CISO on matters related to statewide information security policies and standards.

5.4 BU Director shall:

b. Be responsible for the correct and thorough completion of BU PSPs;

c. Identify and convey contingency planning needs;

d. Ensure compliance with BU PSPs; and

e. Promote efforts within the BU to establish and maintain effective use of agency systems and assets.

5.5 The BU CIO shall:

a. Work with the BU Director to ensure the correct and thorough completion of Agency Information Security PSPs within the BU;

b. Assign the necessary resources to document, implement, and maintain the contingency plan, including the following roles;

c. Recommend/Ensure continuity plans are documented in the contingency plan;

d. Approve developed and modified contingency plan; and

e. Ensure Contingency Planning Policy is periodically reviewed and updated to reflect changes in requirements.

5.6 BU Information Security Officer (ISO) shall:

a. Advise the BU CIO on the completeness and adequacy of the BU activities and documentation provided to ensure compliance with BU Information Security PSPs;

b. Ensure the development and implementation of adequate controls enforcing the Contingency Planning Policy for the BU;

c. Ensure all personnel understand their responsibilities with respect to business continuity and disaster recovery planning; and

d. Work with project leaders on security and privacy related issues involving the development, maintenance, or testing of the contingency plan.

5.7 System owners shall:

a. Participate in establishing, approving, and maintaining policies for the protection controls applicable to the agency systems under their control; and

b. Work with the project leader on agency system related issues involving the development, maintenance, or testing of the contingency plan.

5.8 Supervisors of agency employees and contractors shall:

a. Ensure users are appropriately trained and educated on the Contingency Planning Policy; and

b. Monitor employee activities to ensure compliance.

5.9 System Users of agency systems shall:

- **a.** Become familiar with this policy and related PSPs; and
- **b.** Adhere to PSPs regarding the Contingency Planning Policy.

6. STATEWIDE POLICY

6.1 Develop Contingency Plan – The BU shall develop a contingency plan that: [National Institute of Standards and Technology (NIST) 800-53 CP-2] [Health Insurance Portability and Protection Act (HIPAA) 164.308(a)(7)(i), 164.308(a)(7)(ii)(b), 164.308(a)(7)(ii)(c), 164.310(a)(2)(i)]

- **a.** Identifies essential mission and business functions and the associated contingency requirements consistent with *Establishing an Essential Records List* published by Arizona State Library, Archives and Public Records;
- **b.** Provides recovery objectives, restoration priorities, and metrics;
- **c.** Addresses contingency roles, responsibilities, assigned individuals with contact information;
- **d.** Addresses maintaining essential missions and business functions despite a system disruption, compromise, or failure;
- **e.** Addresses eventual, full systems restoration without deterioration of the controls originally planned and implemented;
- **f.** (P) Addresses resumption of essential missions and business functions within a time frame specified by the BU CIO and based on mission needs, applicable regulations, Arizona State Library, Archives and Public Records requirements and applicable contracts and agreements with external BUs or other organizations. [NIST 800-53 CP-2(3)];
- **g.** (P) Identifies critical assets supporting organizational missions and business functions; [NIST 800-53 CP-2(8)][HIPAA 164.308(a)(7)(ii)(E)]; and
- **h.** (P) Includes procedures for obtaining necessary electronic protected health information during an emergency [HIPAA 164.312(a)(2)(ii)].

6.2 Manage Contingency Plan - The BU shall: [NIST 800-53 CP-2]

- **a.** Distribute the contingency plan to key contingency personnel and organizational elements;
- **b.** Coordinate contingency planning activities with incident handling activities;
- **c.** Review the contingency plan annually;

d. Revise the contingency plan to address changes to the organization, agency systems, operational environment or problems encountered during plan implementation, execution or testing;

e. Communicate contingency plan changes to key contingency personnel and organizational elements; and

f. Protect the contingency plan from unauthorized disclosure and modification.

6.3 (P) **Contingency Plan Coordination** - The BU shall coordinate the development of the contingency plan for each agency system with organizational elements responsible for related plans. [NIST 800-53 CP-2(1)]

6.4 Contingency Training - The BU shall provide contingency training to agency system users consistent with assigned roles and responsibilities before authorizing access, when required by agency system changes, and annually thereafter. The BU shall update and review contingency training content annually, and following a major incident. [NIST 800-53 CP-3]

6.5 Test Contingency Plan - The BU shall test the contingency plan for the agency system annually to determine the effectiveness of the plan and the organizational readiness to execute the plan, review the contingency plan test results, and initiate corrective action. [NIST 800-53 CP-4][HIPAA 164.308 (a)(7)(ii)(D)]

6.5.1 (P) **Contingency Plan Test Coordination** - The BU shall coordinate contingency plan testing for each agency system with organizational elements responsible for related plans. [NIST 800-53 CP-4(1)] [IRS Pub 1075]

6.6 (P) **Alternate Storage Site** - The BU shall establish an alternate storage site including necessary agreements to permit the storage and recovery of system backup information and ensure that the alternative storage site provides information security safeguards equivalent to those of the primary storage site. [NIST 800-53 CP-6]

6.6.1 (P) **Separation from Primary Storage Site** - The alternative storage site shall be separated from the primary storage site to reduce susceptibility to the same hazards. [NIST 800-53 CP-6(1)] [IRS Pub 1075]

6.6.2 (P) **Accessibility** - The BU shall identify potential accessibility problems to the alternate storage site in the event of an area-wide disruption or disaster and outline explicit mitigation actions. [NIST 800-53 CP-6(3)] [IRS Pub 1075]

6.6.3 Arizona State Library, Archive and Public Records is an alternative site by statute (A.R.S. 41-151.12)

6.7 (P) **Alternate Processing Site** - The BU shall: [NIST 800-53 CP-7] [IRS Pub 1075]

a. Establish an alternate processing site including necessary agreements to permit the transfer and resumption of agency system operations for essential missions/business functions with the BU's defined time period consistent with recovery time and recovery point objectives when the primary process capabilities are unavailable;

b. Ensure that equipment and supplies to transfer and resume operations are available at the alternate site or contracts are in place to support delivery to the site in time to support the BU defined period for transfer/resumption; and

c. Ensure that the alternate processing site provides information security safeguards equivalent to that of the primary site.

6.7.1 (P) **Separation from Primary Site** - The BU shall identify an alternative processing site that is separated from the primary site to reduce susceptibility to the same threats. [NIST 800-53 CP-7(1)] [IRS Pub 1075]

6.7.2 (P) **Accessibility** - The BU shall identify potential accessibility problems to the alternate processing site in the event of an area-wide disruption or disaster and outline explicit mitigation actions. [NIST 800-53 CP-7(2)] [IRS Pub 1075]

6.7.3 (P) **Priority of Service** - The BU shall develop alternative processing site agreements that contain priority of service provisions in accordance with the organization's availability requirements. [NIST 800-53 CP-7(3)] [IRS Pub 1075]

6.8 (P) **Alternate Telecommunication Site** - The BU shall ensure alternate telecommunications services are established including necessary agreements to permit the resumption of agency system operations for essential missions and business functions within the BU's defined time period when the primary telecommunication capabilities are unavailable at either the primary or alternate processing or storage sites. [NIST 800-53 CP-8] [IRS Pub 1075]

6.8.1 (P) **Priority of Service Provisions** - The BU shall ensure primary and alternate telecommunications service agreements are developed that contain priority-of-service provisions in accordance with the BU's availability requirements and requests telecommunication service priority for all telecommunications services used for National or State security emergency preparedness in the event that the primary and/or alternate telecommunications services are provided by a common carrier. [NIST 800-53 CP-8 (1)] [IRS Pub 1075]

6.8.2 (P) **Single Points of Failure** - The BU shall ensure alternate telecommunications services are obtained, with consideration for reducing the likelihood of sharing a single point of failure with primary telecommunication services. [NIST 800-53 CP-8(2)] [IRS Pub 1075]

6.9 System Backup - The BU shall: [NIST 800-53 CP-9] [HIPAA 164.308(7)(ii)(A)]

a. Conduct backups of user-level and system-level information contained in the agency system, and agency system documentation including security and privacy related documentation within the BU's defined frequency consistent with recovery time and recovery point objectives; and

b. Protect the confidentiality, integrity, and availability of the backup information.

6.9.1 (P) **Testing for Reliability/Integrity** - The BU shall test backup information at least annually to verify media reliability and information integrity. [NIST 800-53 CP-9(1)] [IRS Pub 1075]

6.9.2 (P) **Cryptographic Protection** - The BU shall implement cryptographic mechanisms to prevent unauthorized disclosure and modification of BU-defined backup information. [NIST 800-53 CP-9(8)]

6.10 system Recovery and Reconstitution - The BU shall provide for the recovery and reconstitution of the agency system to a known state within the BU-defined recovery time and recovery point objectives after a disruption, compromise, or failure. [NIST 800-53 CP-10]

6.10.1 (P) **Transaction Recovery** - The BU shall implement agency systems to perform transaction recovery for any system that is transaction-based. [NIST 800-53 CP-10(2)] [IRS Pub 1075]

7. DEFINITIONS AND ABBREVIATIONS

7.1 Refer to the PSP Glossary of Terms located on the ADOA-ASET and NIST Computer Security Resource Center websites.

8. REFERENCES

8.1 STATEWIDE POLICY FRAMEWORK 8230 Contingency Planning

8.2 Statewide Policy Exception Procedure

8.3 National Institute of Standards and Technology, Special Publication 800-53 Revision 5, Security and Privacy Controls for Information Systems and Organizations, September 2020.

8.4 HIPAA Administrative Simplification Regulation, Security and Privacy, CFR 45 Part 164, February 2006

8.5 IRS Publication 1075, Tax Information Security Guidelines for Federal, State, and Local Agencies: Safeguards for Protecting Federal Tax Returns and Return Information, 2021.

8.6 Establishing an Essential Records List, Arizona State Library, Archives and Public Records

8.7 General Records Retention Schedule Issued to All Public Bodies, Management Records, Schedule Number: GS 1005, Arizona State Library, Archives and Public Records, Item Number 7

8.8 A.R.S. 41-151.12

9. ATTACHMENTS

None.

10. REVISION HISTORY

Date	Change	Revision	Signature
9/01/2014	**Initial release**	**Draft**	**Aaron Sandeen, State CIO and Deputy Director**
10/11/2016	**Updated all the Security Statutes**	**1.0**	**Morgan Reed, State CIO and Deputy Director**
9/17/2018	**Updated for PCI-DSS 3.2.1**	**2.0**	**Morgan Reed, State of Arizona CIO and Deputy Director**
5/26/2021	**Annual Updates**	**3.0**	**Tim Roemer, Director of Arizona Department of Homeland Security & State Chief Information Security Officer**
12/19/2023	**Annual Updates**	**4.0**	**Ryan Murray, Deputy Director Department of Homeland Security & State Chief Information Security Officer**
1/30/2025 **2/11/2025**	**Annual Updates**	**5.0**	**Errika Celsy, Chief Privacy and Compliance Officer;** **Deputy Director Department of Homeland Security & State Chief Information Security Officer**