ARIZONA DEPARTMENT OF ADMINISTRATION	Agency POLICY	State of Arizona

POLICY 6000: STATE DATA CENTER (SDC) INFRASTRUCTURE CONTINGENCY PLANNING

DOCUMENT NUMBER:	**ADOA– P6000**
EFFECTIVE DATE:	**OCTOBER 11, 2014**
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 minimize the risk of system and service unavailability due to a variety of disruptions by providing effective and efficient solutions to enhance system availability. [National Institute of Standards and Technology (NIST) 800-34]

3. SCOPE

3.1 This policy applies to all Divisions of ADOA and IT integrations and/or data exchange with third parties that perform functions, activities or services for or on behalf of the Agency or its Divisions through the State Data Center (SDC). Applicability of this policy to third parties is governed by contractual agreements entered into between ADOA and the third party/parties.

3.1.1 **Application to Systems** - This policy shall apply to all state information systems. Categorization of systems is defined within Policy 8120, Information Security Program.

3.2 **Application to Third Parties** - This Policy shall apply to all ADOA vendors and contractors providing goods and services to the ADOA and to third parties, including other Government bodies.

4. EXCEPTIONS

4.1 In the event that an incident requiring the temporary relocation of SDC operational capabilities, technologies, systems, or data, SDC will support such relocation activity of agency owned and managed equipment and data. SDC support of such equipment and data will be limited to, and in accordance with, in force contracts related to contingency planning.

5. ROLES AND RESPONSIBITIES

Note: The types of teams required are based on the definition of services available to the agencies.

5.1 State Chief Information Officer (CIO) shall:

a. Be ultimately responsible for the correct and thorough completion of Statewide IT PSPs throughout all state BUs.

5.2 Chief Operating Officer (COO), Assistant Director, State Data Center Manager shall:

a. Oversee the management and operation of the State Data Center;

b. Make decisions, with respect to, the application of State policies and Arizona Revised Statutes to the SDC;

c. Be the ultimate authority to ensure that contracted service delivery and support commitments are met, including but not limited to, making decisions regarding spending levels, acceptable risk, and interagency coordination of service events and decisions requiring their concurrence; and

d. Lead the SDC management team in its accomplishment of specific responsibilities critical to the delivery and support of SDC services.

5.3 ADOA Disaster Recovery Manager shall:

a. Conduct periodic risk assessments, including but not limited to, natural disasters, man-made disasters, and disruptions affecting technology assets.

b. Establish and maintain contingency plans including, but are not limited to, business continuity and incident recovery plans consistent with State policies and A.R.S. § 18-104(c);

c. Collaborate with the ADOA Chief Operating Officer, in the coordination of recovery activities for a declared disaster;

d. Establish and maintain incident recovery education and training programs necessary to ensure the readiness of personnel required to support disaster recovery activities;

e. Conduct periodic reviews and tests of shutdown and recovery procedures, business risks, emergency procedures, and data backup procedures; and

f. Ensure that all contingency plans, including but not limited to, business continuity and incident recovery plans and related documents or artifacts are under configuration change control and integrated with the disruption management process.

6. SDC POLICY

The principal objective of Contingency Planning is to adopt industry best practices to data center operations that will ensure the recovery of departmental and agency functions that must be continued throughout, or resumed after a disruption of normal activities from an unforeseen event, disaster or emergency interrupting information systems and business operations.

6.1 **Business Impact Analysis** (BIA) - SDC shall conduct an annual business impact analysis, with agency BUs, of their information systems. [(NIST) 800-34]

6.1.1 **Identify Supported BU Processes** - SDC shall identify supported BU processes and recovery criticality. Impact to BU processes will be categorized (Low, Moderate, High) for confidentiality, integrity, and availability.(FIPS PUB 199)

6.1.2 **Identify Outage Impacts** - SDC shall identify outage impacts and estimated downtime. Downtime should reflect the maximum time that a BU can tolerate while still maintaining the mission at an acceptable level of service.

6.1.3 **Identify Resource Requirements** - SDC shall identify resource requirements. Recovery efforts require an evaluation of resources required to resume mission/business processes. Resources may include facilities, personnel, equipment, software, data files, system components, and vital records.

6.1.4 **Identify Recovery Priorities** - SDC shall identify recovery priorities for systems. Each system or BU process shall be analyzed and the Maximum Tolerable Downtime (MTD), Recovery Time Objective (RTO), and Recovery Point Objective (RPO) determined for each.

6.2 **Annual Risk Assessment** – SDC shall conduct and document annual risk assessments to identify, estimate, and prioritize risk to BU operations. Risks may include, but are not limited to, natural disasters, man-made disasters, and disruptions caused by information technology assets. Priority will be given to risks that are estimated to have the greatest potential impact and the highest probability of occurrence. [(NIST) 800-30]

6.3 **Risk Management/Business Continuity Plan** - SDC shall manage identified high-priority risks by developing, documenting, and testing a comprehensive Business Continuity Plan. The Business Impact Analysis and Risk Assessment represent the foundation of the Business Continuity Plan. [(NIST) 800-34]

6.3.1 **Identify Preventive Controls** – SDC shall identify preventive controls that address the most significant areas of risk identified by the Risk Assessment. Each preventive control shall be analyzed in terms of effectiveness, practicality and cost effectiveness. Preventive controls identified as effective and efficient will be included in the Business Continuity Plan. [(NIST) 800-34]

6.3.2 **Create Contingency Strategies** – SDC shall identify contingency strategies and alternatives to address high-priority risks. These strategies include, but are not limited to: Backup and recovery of data and; Alternate sites. [(NIST) 800-34]

6.3.2.1 **State Information System Backup** - SDC shall: Conduct backups of data/information contained in the state information system, and state information system documentation including security-related documentation within the SDC's defined frequency consistent with RPO/RTOs defined in contracted SLAs/OLAs; and [NIST 800-53 CP-9] [HIPAA 164.308(7)(ii)(A)]

a) Protect the confidentiality, integrity, and availability of the backup information at storage locations.

6.3.2.1.1 **Testing for Reliability / Integrity** - SDC shall ensure recoverability of data written to media and stored offsite annually to verify media reliability and information integrity. [NIST 800-53 CP-9(1)] [IRS Pub 1075]

6.3.2.1.2 **Information System Recovery and Reconstitution** - SDC, with direction from the data owner, shall provide for the recovery and reconstitution of the state information system after a disruption, compromise, or failure to the contracted RPO. [NIST 800-53 CP-10]

6.3.2.1.3 **Transaction Recovery** – SDC, with direction from the data owner and based on the RPO, shall implement state information systems to perform transaction recovery for any system that is transaction-based. [NIST 800-53 CP-10(2)] [IRS Pub 1075]

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

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

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

6.3.2.2.3 **Priority of Service** - SDC shall develop alternate storage site components as a part of service level agreements (SLAs) and organizational level agreements (OLAs) that specifies storage provisioning in accordance with the organization's availability requirements. [NIST 800-53 CP-7(3)] [IRS Pub 1075]

6.3.2.3 **Alternate Processing Site** - SDC 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 state information system operations for essential missions/business functions with the SDC's defined time period consistent with RPOs and RTOs 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 SDC defined period for transfer/resumption;

c) Ensure all service levels are met while at the alternate data center site, in accordance with agency service agreements and to the best of the secondary site's capabilities, for the duration of the incident; and

d) Ensure that the alternate processing site provides information security safeguards similar or equivalent to that of the primary site.

6.3.2.3.1 **Separation from Primary Site** - SDC 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]

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

6.3.2.3.3 **Priority of Service** - SDC 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]

6.3.3 Incident recovery plan (IRP) – SDC shall develop an Incident Recovery plan that addresses physical disruptions that require relocation of IT equipment, processes, or data storage.

6.3.4 Continuity of Operations Plan (COOP) - SDC shall develop a Continuity of Operations Plan with the BU to insure that mission essential functions (MEF) are restored following disruptions that require relocation of IT equipment, processes, or data storage.

6.3.5 Information System Contingency Plan (ISCP) – SDC shall develop an Information System Contingency Plan that insures all identified BU processes are restored following disruptions that may or may not include relocation of IT equipment, processes, or data storage.

6.3.6 Crisis Management Plan (CMP) SDC shall develop a Crisis Management Plan that includes:

a. A database with names, phone/page/fax/cellular numbers, e-mail and postal addresses of everyone on the team.

b. Assigned roles and procedures for everyone on the crisis team.

c. A multimedia database with critical information on the organization's assets, personnel and services that can be quickly accessed and analyzed.

d. A means for team members to access the database and collaborate remotely.

e. A Crisis Communication Plan that addresses communications with personnel and the public at large.

6.4 Develop Contingency Plans - SDC shall develop contingency plans for each high-priority risk that: [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;

b. Provides Recovery Point Objective (RPO) and Recovery Time Objective (RTO) restoration priorities and metrics based on Service Level Agreements (SLA);

c. Addresses contingency roles, responsibilities, assigned individuals with contact information;

d. Addresses maintaining essential missions and business functions despite an information system disruption, compromise, or failure;

e. Addresses eventual, full information systems restoration without deterioration of the security safeguards originally planned and implemented;

f. Addresses resumption of essential missions and business functions within a time frame specified by the ADOA CIO and based on mission needs, applicable regulations, and applicable contracts and agreements with external BUs or other organizations. [NIST 800-53 CP-2(3)];

g. Identifies critical information system assets supporting organizational missions and business functions; [NIST 800-53 CP-2(8)][HIPAA 164.308(a)(7)(ii)€];

h. Includes procedures for obtaining necessary electronic protected health information during an emergency [HIPAA 164.312(a)(2)(ii)]; and

i. Is reviewed and approved by ADOA COO and Assistant Director/State Data Center Manager.

6.4.1 Contingency Plan Coordination - SDC shall recommend and coordinate the development of the contingency plan for each state information system with organizational elements responsible for related plans. [NIST 800-53 CP-2(1)] [Internal Revenue Service (IRS) Pub 1075]

6.5 Contingency Training - SDC shall provide contingency training to state information system users consistent with assigned roles and responsibilities before authorizing access, when required by state information system changes, and annually thereafter. [NIST 800-53 CP-3]

6.6 Test Contingency Plan - SDC shall test the contingency plan for the state information 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 or improvements, as necessary. [NIST 800-53 CP-4][HIPAA 164.308(a)(7)(ii)(D)]

6.6.1 Contingency Plan Test Coordination - SDC shall coordinate contingency plan testing for each state information system with organizational elements responsible for related plans. [NIST 800-53 CP-4(1)] [IRS Pub 1075]

6.7 Manage Contingency Plans - SDC shall: [NIST 800-53 CP-2]

- **a.** Distribute contingency plans to key SDC support personnel, and appropriate SDC service providers and partners;
- **b.** Coordinate contingency planning activities with incident handling activities;
- **c.** Review contingency plans annually based on the annual Risk Assessment and any changes in the Business Impact Analysis to insure that it comprehensively addresses all high-priority risks;
- **d.** Revise contingency plans as necessary to address changes to the organization, state information 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 contingency plans from unauthorized disclosure and modification.

7. DEFINITIONS AND ABBREVIATIONS

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

8. REFERENCES

8.1 Statewide Policy Framework P100, Information Technology

8.2 Statewide Policy Framework 8120, Information Security Program

8.3 National Institute of Standards and Technology (NIST) Special Publication 800-30 (SP800-30). Guide for Conducting Risk Assessments

8.4 National Institute of Standards and Technology (NIST) Special Publication 800-34 Rev. 1 (SP800-34). Contingency Planning Guide for Federal Information Systems

8.5 National Institute of Standards and Technology (NIST) Special Publication 800-53 Rev. 4 (SP800-53). Recommended Security Controls for Federal Information Systems

8.6 National Institute of Standards and Technology (NIST) Special Publication 800-84 (SP800-84). Guide to Test, Training, and Exercise Programs for IT Plans and Capabilities

8.7 Federal Emergency Management Agency (FEMA) Continuity Guidance Circular 1 (CGC1), Continuity Guidance for Non-Federal Entities (States, Territories, Tribal, and Local Government Jurisdictions and Private Sector Organizations), January 21, 2009

8.8 Federal Emergency Management Agency (FEMA) National Response Framework (NRF), 2nd Edition, May 2013.

9. ATTACHMENTS

None.

10. REVISION HISTORY

Date	Change	Revision	Signature
07/10/2014	Initial Release	1.0	Aaron Sandeen, State CIO and Deputy Director
10/11/2016	Updated all the Security Statutes	1.0	Morgan Reed, State CIO and Deputy Director