ARIZONA **D**EPARTMENT **O**F **A**DMINISTRATION	**STATEWIDE** **POLICY**	**State of Arizona**

STATEWIDE POLICY (8240): INCIDENT RESPONSE PLANNING

DOCUMENT NUMBER:	**(P8240)**
EFFECTIVE DATE:	**SEPTEMBER 17, 2018**
REVISION:	**2.0**

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 and § 18-105. REFERENCE STATEWIDE POLICY FRAMEWORK 8240 INCIDENT RESPONSE PLANNING.

2. PURPOSE

The purpose of this policy is to increase the ability of the Budget Unit (BU) to rapidly detect incidents, minimize any loss due to destruction, mitigate the weaknesses that were exploited, and restore computing services.

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 information systems:

a. (P) Policy statements preceded by "(P)" are required for agency information systems categorized as Protected.

b. (P-PCI)Policy statements preceded by "(P-PCI)" are required for agency information systems with payment card industry data (e.g., cardholder data).

c. (P-PHI) Policy statements preceded by "(P-PHI)" are required for agency information systems with protected healthcare information.

d. (P-FTI) Policy statements preceded by "(P-FTI)" are required for agency information systems with federal taxpayer information.

3.3 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 IT 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 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 State Chief Information Security Officer (CISO) shall:

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

b. Review and approve or disapprove all state BU security and privacy PSPs and exceptions to existing PSPs; and

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

5.3 State Chief Privacy Officer (CPO) shall:

a. Advise the State CIO and the State CISO on the completeness and adequacy of the BU activities and documentation for data privacy provided to ensure compliance with Statewide Information Technology Privacy PSPs throughout all state BUs;

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

c. Identify and convey to the State CIO and the State CISO the privacy risk to state information systems and data based on current implementation of privacy controls and mitigation options to improve privacy.

5.4 BU Director shall:

a. Be responsible for the correct and thorough completion of (Agency) BU PSPs;

b. Ensure compliance with BU PSPs with Incident Response Planning Policy; and

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

5.5 BU CIO shall:

a. Work with the BU Director to ensure the correct and thorough completion of BU IT PSPs; and

b. Ensure BU PSPs are periodically reviewed and updated to reflect changes in requirements, lessons learned from actual incidents, and advances the industry.

5.6 BU 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 Technology PSPs;

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

c. Ensure all personnel understand their responsibilities with respect to planning and responding to security incidents.

5.7 BU Privacy Officer shall: [EO 2008-10]

a. Advise the State CISO and the State CPO on the completeness and adequacy of the BU activities and documentation provided to ensure compliance with privacy laws, regulations, and statutes; and

b. Assist the agency to ensure the privacy of sensitive personal information within the agency's possession.

5.8 Supervisors of agency employees and contractors shall:

a. Ensure users are appropriately trained and educated on Incident Response Planning Policy; and

b. Monitor employee activities to ensure compliance.

5.9 System Users of agency information systems shall:

a. Become familiar with this policy and related PSPs; and

b. Adhere to PSPs regarding classification of incidents response planning within agency information systems.

6. STATEWIDE POLICY

6.1 **Incident Response Training** - The BU shall provide incident response training to agency information system users consistent with assigned roles and responsibilities before authorizing access to the agency information system or performing assigned duties, when required by agency information system changes, and annually thereafter. [NIST 800-53 IR-2] [IRS Pub 1075] [PCI DSS 12.10.4]

6.2 (P) **Incident Response Testing** – The BU shall test the incident response capability for the agency information system annually using checklists, walk-through, tabletop exercises, simulations or comprehensive exercises to determine the incident response effectiveness and document the results. [NIST 800-53 IR-3] [IRS Pub 1075] [PCI DSS 12.10.2]

6.2.1 (P) **Coordinated Testing** – The BU shall coordinate incident response testing with BU elements responsible for related plans. [NIST 800-53 IR-3(2)] [IRS Pub 1075]

6.2.2 **(P) Incident Response Test Elements** – The BU shall include the following elements (at a minimum) in the annual incident response test: [PCI DSS 12.10.2]

c. Incident response roles and responsibilities, communications, and contact strategies

d. Specific incident response procedures

e. Business recovery and continuity procedures

f. Data back-up processes

g. Legal requirement and breach notification analysis

h. Critical system component coverage and responses

i. Reference or inclusion of Incident response procedures from external entities

6.3 Incident Handling - The BU shall implement an incident handling capability for security incidents that includes: [NIST 800-53 IR-4] [IRS Pub 1075] [HIPAA 164.308(a)(6)(ii)] [PCI DSS 12.10.1]

a. Preparation, detection and analysis, containment, eradication, and recovery;

b. Incident handling activities with contingency planning activities; These activities shall address the following at a minimum:

- Unauthorized wireless access point detection [PCI DSS 11.1.2]
- Alerts generated by change detection solutions (e.g., unauthorized modification of critical files, configuration files or content files) [PCI DSS 11.5.1]

c. Incident response procedures, training, and testing/exercises covering industry developments and lessons learned from ongoing incident handling activities that drive the modification and evolution of the incident response plan; [PCI 12.10.6]

d. Industry developments; and

e. Implementation of industry development changes where applicable.

6.3.1 (P) **Automated Incident Handling Processes** - The BU shall employ automated mechanisms to support the incident handling process. [NIST 800-53 IR-4(1)] [IRS Pub 1075]

6.3.2 (P) **Assign Incident Handling Role** - The BU shall assign to an individual or team the information security management responsibility of implementing an incident response plan and to be prepared to respond immediately to a system breach. [PCI DSS 12.10.1]

6.3.3 (P-PCI) **24x7 Availability** - The BU shall assign to specific personnel the information security management responsibility of being available on a 24x7 basis to respond to alerts. [PCI DSS 12.10.3]

6.3.4 (P) **Forensic Capability** - For agencies that provide a shared hosting service, the BU shall establish processes to provide for timely forensic investigation in the event of a compromise to any hosted service. [PCI DSS A.1.3]

6.4 (P) **Privacy Incident Response Handling** – The BU shall provide an organized and effective response to privacy incidents in accordance with the BU Privacy Incident Response Plan. [NIST 800-53 SE-2]

6.5 Incident Monitoring - The BU shall track and document agency information system security incidents. [NIST 800-53 IR-5] [IRS Pub 1075] [HIPAA 164.308(a)(6)(ii)]

6.5.1 (P) **Assign Incident Monitoring Role** - The BU shall assign to an individual or team the information security management responsibility of monitoring and analyzing security alerts and information and distributing alerts to appropriate personnel. [PCI DSS 12.5.2]

6.5.2 (P) **Incorporate Automated Alerts** - The BU shall implement the system to include alerts from intrusion detection, intrusion prevention, and file integrity monitoring systems. [PCI DSS 12.10.5]

6.6 Incident Reporting - The BU shall require personnel to report: [NIST 800-53 IR-6] [ARS 41-3507] [IRS Pub 1075] [EO 2008-10] [HIPAA 164.308(a)(6)(ii)] [HIPAA 164.308(a)(1)(ii)(D)] [HIPAA 164.314(a)(2)(i)(C)]

a. Suspected security incidents to the organizational incident response capability within one hour of knowledge of suspected incident as specified in the Statewide Standard 8240, Incident Response Planning:

1. (In the event of a security incident) Security incident information to the State CISO; and

2. (In the event of a privacy incident) Privacy incident information to the State Privacy Officer.

6.6.1 Use of Statewide Incident Handling Program – BUs utilizing the statewide incident handling program meet the requirement for reporting of security and privacy incidents that are visible within the program (e.g., part of the monitored systems and logs). However, BUs must implement a system to integrate the notification process for security incidents that originate outside of the monitored systems (e.g., employee reported malware, onsite physical threats, reported loss of laptop). [ARS 41-2507]

6.6.2 (P) **Automated Incident Reporting** - The BU shall employ automated mechanisms to assist in the reporting of security incidents. [NIST 800-53 IR-6(1)] [IRS Pub 1075]

6.7 Incident Response Plan - The BU shall: [NIST 800-53 IR-8] [IRS Pub 1075] [PCI DSS 12.10, 12.10.1]

a. Develop an incident response plan that:

1. Provides the organization with a roadmap for implementing its incident response capability;

3. Describes the structure and organization of the incident response capability;

2. Provides a high-level approach for how the incident response capability fits into the overall organization;

3. Meets the unique requirements of the organization, which relate to mission, size, structure, and functions;

4. Defines reportable incidents;

5. Provides metrics for measuring the incident response capability within the organization;

6. Defines the resources and management support needed to effectively maintain and manage an incident response capability;

7. (P-PCI) Describes the roles, responsibilities, and communication and contact strategies in the event of a compromise including notification of the payment brands, specific incident response procedures, business recovery and continuity procedures, data backup processes, analysis of legal requirements for reporting compromises, coverage and responses of all critical system components, and reference or inclusion of incident response procedures from the payment brands. [PCI DSS 12.10.1]; and

8. Is reviewed and approved by the BU Information Security Officer.

b. Distribute copies of the incident response plan to incident response personnel and organizational elements;

c. Review the incident response plan annually;

d. Revise the incident response plan to address system/organizational changes or problems encountered during plan implementation, execution, or testing; and

e. Communicate incident response plan changes to (Agency) BU incident response personnel and the State CISO and State Privacy Officer.

6.8 Incident Response Assistance - The BU shall provide an incident response support resource, integral to the BU incident response capability that offers advice and

assistance to users of the information system for the handling and reporting of security incidents. [NIST 800-53 IR-7] [IRS Pub 1075]

6.8.1 (P) **Automated Support for Availability of Information** - The BU shall employ automated mechanisms to increase the availability of incident response-related information and support. [NIST 800-53 IR-7(1)] [IRS Pub 1075]

6.9 (P) **Privacy Incident Response Plan** - The BU shall develop and implement a Privacy Incident Response Plan. [NIST 800-53 SE-2]

6.9.1 **Investigation** - The BU shall investigate potential privacy incidents upon awareness of unencrypted Personally Identifiable Information (PII) loss. [ARS 44-7501]

6.9.2 **Notification** – The BU shall notify affected parties upon breach determination without unreasonable delay. [ARS 44-7501]

a. Non-state Owned PII Notification - For PII not owned by the state, the BU shall notify and cooperate with the owner following the discovery of a breach without unreasonable delay. [ARS 44-7501]

b. Notification Exceptions - The BU may delay notification if law enforcement determines notification will impede the investigation. [ARS 44-7501]

c. Notification Methods - The BU may use telephone, electronic notice, or email as a method of notification. [ARS 44-7501]

7. DEFINITIONS AND ABBREVIATIONS

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

8. REFERENCES

8.1 STATEWIDE POLICY FRAMEWORK 8240 Incident Response Planning

8.2 Statewide Standard 8240, Incident Response Planning

8.3 Statewide Policy Exception Procedure

8.4 Incident Handling Program

8.5 NIST 800-53 Rev. 4, Recommended Security Controls for Federal Information Systems and Organizations, February 2013.

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

8.7 Payment Card Industry Data Security Standard (PCI DSS) v3.2.1, PCI Security Standards Council, May 2018.

8.8 IRS Publication 1075, Tax Information Security Guidelines for Federal, State, and Local Agencies: Safeguards for Protecting Federal Tax Returns and Return Information, 2010.

8.9 Executive Order 2008-10: Mitigating Cyber Security Threats, January 14, 2008.

9. ATTACHMENTS

None.

10. REVISION HISTORY

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 Rees, State CIO and Deputy Director**