STATEWIDE POLICY (8240): INCIDENT RESPONSE PLANNING

DOCUMENT NUMBER:	**P8240**
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 (A.R.S.)§ 41-4254 and § 41-4282.

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 systems:

- **a. (P)** Policy statements preceded by "(P)" are required for agency systems categorized as Protected.
- **b. (P-PCI)**Policy statements preceded by "(P-PCI)" are required for agency systems with payment card industry data (e.g., cardholder data).
- **c. (P-PHI)** Policy statements preceded by "(P-PHI)" are required for agency systems with protected healthcare information.
- **d. (P-FTI)** Policy statements preceded by "(P-FTI)" are required for agency 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 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 or disapprove all state BU security and privacy PSPs and exceptions to existing 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 State Chief Privacy Officer (CPO) shall:

a. Advise the Director 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 security and 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 Director and the State CISO the privacy risk to state systems and data based on current implementation of privacy controls and mitigation options to improve privacy.

5.4 Enterprise Security Program Advisory Council (ESPAC)

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

5.5 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 systems and assets.

5.6 BU CIO shall:

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

5.7 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 Security 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.

5.8 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.

5.9 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.

5.10 System users of agency systems shall:

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

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

6. STATEWIDE POLICY

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

6.1.1 Breach - The BU shall provide incident response training on how to identify and respond to a breach, including the organization's process for reporting a breach. [NIST 800-53 IR-2(3)]

6.2 (P) Incident Response Testing – The BU shall test the incident response capability for the agency 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]

- **a.** Incident response roles and responsibilities, communications, and contact strategies
- **b.** Specific incident response procedures
- **c.** Business recovery and continuity procedures
- **d.** Data back-up processes
- **e.** Legal requirement and breach notification analysis
- **f.** Critical system component coverage and responses
- **g.** Reference or inclusion of Incident response procedures from external entities

6.3 Incident Handling - The BU shall implement an incident handling capability for incidents that is consistent with the incident response plan, and; [NIST 800-53 IR-4] [IRS Pub 1075] [HIPAA 164.308(a)(6)(ii)] [PCI DSS 12.10.1] [PCI DSS 107.3]

- **a.** The BU incident response plan shall include preparation, detection and analysis, containment, eradication, and recovery;
- **b.** The BU shall coordinate incident handling activities with contingency planning activities; These activities shall address the following at a minimum:
  1. Unauthorized wireless access point detection [PCI DSS 11.1.2]
  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.** The incident response procedures, training, and testing/exercises shall cover 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]industry developments;
- **d.** Implementation of industry development changes where applicable; and
- **e.** The BU shall ensure the rigor, intensity, scope, and results of incident handling activities are comparable and predictable across the organization.

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

6.4.1 (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]

6.4.2 (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]

6.4.3 **Continuous Monitoring Strategy** - The BU shall develop an BU-wide continuous monitoring strategy and implement continuous monitoring programs that include: [NIST 800 53 PM-31]

- **a.** Establishing the BU-defined metrics to be monitored;
- **b.** Establishing BU-defined frequency for monitoring and annual assessment of control effectiveness;
- **c.** Ongoing monitoring of BU-defined metrics in accordance with the continuous monitoring strategy;
- **d.** Correlation and analysis of information generated by control assessments and monitoring;
- **e.** Response actions to address results of the analysis of control assessment and monitoring information; and
- **f.** Reporting the security and privacy status of BU systems to the BU CISO, BU Privacy Officer, State CISO and State Privacy Officer annually.

6.5 Incident Reporting - The BU shall require personnel to report: [NIST 800-53 IR-6] [ARS 41-4282] [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:
- **b.** (In the event of a security incident) Security incident information to the State CISO; and
- **c.** (In the event of a privacy incident) Privacy incident information to the State Privacy Officer.

6.5.1 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).

6.5.2 (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]

6.5.3 (P) **Supply Chain Coordination** - The BU shall provide incident information to the provider of the product or service and other organizations involved in the supply chain or supply chain governance for systems of system components related to the incident. [NIST 800-53 IR-6(3)]

6.5.4 (P) **Incident Response Reporting** - the BU shall respond to information spills by: [NIST 800 53 IR-9]

- **a.** Assigning [Assignment: organization-defined personnel or roles] with responsibility for responding to information spills;
- **b.** Identifying the specific information involved in the system contamination;
- **c.** Alerting authorized incident response personnel of the information spill using a method of communication not associated with the spill;
- **d.** Isolating the contaminated system or system component;
- **e.** Eradicating the information from the contaminated system or component;
- **f.** Identifying other systems or system components that may have been subsequently contaminated; and
- **g.** Performing the additional BU-defined actions.

6.6 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;
2. Describes the structure and organization of the incident response capability;
3. Provides a high-level approach for how the incident response capability fits into the overall organization;
4. Meets the unique requirements of the organization, which relate to mission, size, structure, and functions;
5. Defines reportable incidents;
6. Provides metrics for measuring the incident response capability within the organization;
7. Defines the resources and management support needed to effectively maintain and manage an incident response capability;
8. (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
    i. Is reviewed and approved by the BU Information Security Officer;
    ii. Addresses the sharing of incident information;
    iii. Explicitly designates the responsibility for incident response.
9. (P) Addresses breaches involving confidential identifiable information. including: a process to determine if notice to individuals or other organizations, including oversight organizations, is needed; an assessment process to determine the extent of the harm, embarrassment, inconvenience, or unfairness to affected individuals and any mechanisms to mitigate such harms; and identification of applicable privacy requirements. [NIST 800-53 IR-8(1)] [PCI DSS 12.10.7]

b. The BU shall:
1. Distribute copies of the incident response plan to incident response personnel and organizational elements;
2. Review the incident response plan annually;
3. Revise the incident response plan to address system/organizational changes or problems encountered during plan implementation, execution, or testing;

4. Communicate incident response plan changes to (Agency) BU incident response personnel and the State CISO and State Privacy Officer; and
5. Protect the incident response plan from unauthorized disclosure and modification.

6.7 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 system for the handling and reporting of incidents. [NIST 800-53 IR-7] [IRS Pub 1075]

6.7.1 (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]

6.8 Investigation - The BU shall promptly investigate potential privacy incidents upon awareness of unencrypted Personally Identifiable Information (PII) loss. [ARS 18-552.A]

a. Breach Determination – The investigation shall determine if the security incident resulted in a system security breach. [ARS 18-552.A]

b. Determination of No Substantial Economic Loss – If an independent third-party forensic auditor or law enforcement agency performed a reasonable investigation and has determined that the system breach has not resulted in or is not reasonably likely to result in substantial economic loss to affected individuals the BU is not required to make the notification as described below. [ARS 18-552.J]

6.9 Notification – The BU shall notify affected parties upon breach determination within 45 days after the determination. [ARS 18-551.B, 18-551.H][HIPAA 164.404(a)]

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 as soon as practicable, including sharing information relevant to the breach. [ARS 18-552.C]

b. Notification Exceptions - The BU may delay or potentially forgo notification in the following cases:

1. If law enforcement determines notification will impede the investigation. The required notification shall be implemented within 45 days of being informed by law enforcement that notifications no would longer impede the investigation, [ARS 18-552.D] [HIPAA 164.412]
2. Good Faith Exposure – No notification is required in the event the disclosure was unintentional or inadvertent by a workforce

member acting in good faith and there is no further disclosure. [HIPAA 164.402.1.i-ii]

3. No Retention – No notification is required in the event the disclosure is to an unauthorized person but it is believed that there is no reasonable way for that person to retain the information. [HIPAA 164.402.1.iii]
4. Low Probability of Compromise – No notification is required in the event the disclosure is demonstrated to have a low probability of compromise based on a risk assessment that considers at least the following factors: [HIPAA 164.402.2]
    i. The nature and extent of the PHI involved (including identifier types, and likelihood of re-identification);
    ii. The unauthorized person to whom the PHI was exposed;
    iii. Whether the PHI was actually acquired or viewed; and
    iv. The extent to which the risk to the PHI has been mitigated.
5. If the BU determines a low probability of compromise the determination must be supported through a documented risk analysis process. [See attachment for Example Harm Analysis]

c. Notification Methods - The BU may use written notice via mail, telephone (but not through a prerecorded message), or email as a method of notification. [ARS 18-552.F]

1. If the cost of notification via these methods would exceed $50,000 the notification method may be a written letter to the Attorney General that demonstrates the facts necessary for substitute notice, and a conspicuous posting of the notice for at least 435 days on the BU website. [ARS 18-552.F.4]
2. If the breach involves account login information (e.g., username and password or security questions) and not any other personal information, the notification may an electronic message that directs the user to re-secure the account (and all other accounts using the same password or security question) by changing the password and security question(s). [ARS 18-551.G]

3. If the breach involves account login information with an email account the notification may be directed to the individual using a method other than the suspect email address:
    i. Notification delivered online when the IP address or online location matches a known customary address or location for that account. [ARS 18-551.G]

d. (P-PHI) Notification Timing – The BU shall implement notifications without unreasonable delay and in no case later than 45 days after discovery of a breach or suspected breach of PHI. [ARS 18-552.B], [HIPAA 164.404(b), 164.406(b)]

e. Notification Elements – The notification shall include the following elements: [ARS 18-552.E]

1. Approximate date of breach;
2. Brief description of personal information included in the breach;
3. Toll-free numbers and addresses for the 3 largest nationwide consumer reporting agencies, and;
4. Toll-free number, address and website address for the federal trade commission or any federal agency that assists consumers with identity theft matters.

f. (P-PHI) Additional Notifications – For a breach of unsecured PHI the following additional notifications must be implemented:

1. Breach Log - For breaches involving less than 500 residents of a State or jurisdiction the BU shall maintain a log of such breaches; [HIPAA 164.408(c)].
2. Media Notification - For PHI breaches involving more than 500 residents of a State or jurisdiction the BU shall notify prominent media outlets serving the State or jurisdiction; [HIPAA 164.406(a)].
3. (P-PII) Media Notification – For PII breaches involving more than 1000 individuals notify the 3 largest nationwide consumer-reporting agencies and the attorney general with a copy of the notification provided to the individuals; [A.R.S. 18-552.B.2]
4. HHS Secretary Notification – For any PHI breach the BU shall notify the Secretary of Health and Human Services. In addition each year the BU shall notify the HHS Secretary of the logged

data of PHI breaches in the manner specified on the HHS website. [HIPAA 164.408(a), 164.408(b), 164.408(c)].

g. (P) Federal Regulators – A BU is compliant with the notification requirements if they are compliant with the notification requirements established by their primary or functional federal regulator. [ARS 18-552.I]

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

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

8.7 HIPAA HITECH (Health Information Technology for Economic and Clinical Health) Act February 17, 2010.

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

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

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

9. ATTACHMENTS

Example Risk of Harm Analysis Procedure:
https://aset.az.gov/resources/policies-standards-and-procedures

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**