ARIZONA STATEWIDE SECURITY STANDARD	STATEWIDE STANDARD	State of Arizona

STANDARD 8240: INCIDENT RESPONSE PLANNING

DOCUMENT NUMBER:	S8240
EFFECTIVE DATE:	May 26, 2021
REV:	3.0

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.

2. PURPOSE

The purpose of this standard is to provide additional specificity to the associated policy requirements.

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** - The policy shall apply to all state information systems. Policy statements preceded by “(P)” are required for state information systems categorized as Protected. Categorization of systems is defined within the Information Security Program Policy.

4. EXCEPTIONS

None.

5. ROLES AND RESPONSIBILITIES

See section 5 of P8240 Incident Response Policy.

6. STATEWIDE STANDARD

6.1 **Incident Response Team Training** - The BU shall provide incident response team training that ensures the team is adequately prepared to handle a variety of incidents.

6.1.1 Incident Response Team Training - The incident response team shall be provided adequate training to ensure they are familiar with the incident response plan and procedures, their role and responsibilities, and the appropriate skills to perform their duties.

6.1.2 Lessons Learned - The incident response team shall conduct lessons learned meetings as a means to improve the incident response capability. The purpose of the lessons learned meeting is to review the effectiveness of the current incident response capabilities, documented processes, and usefulness of these processes to assist and guide the team members in handling the incident.

a. **Frequency** - After major incidents have been resolved and periodically for lesser incidents the incident response team lead shall conduct a Lessons Learned meeting.

b. **Attendance** – The Lessons Learned meeting should include as many team members as possible.

c. **Objectives** - The objectives of the Lessons Learned meeting is to identify, document, and correct systemic weaknesses and deficiencies in the policies and procedures.

d. **Documentation** - The Lessons Learned meeting, findings, and action items shall be documented. If the BU has a ticketing system in place, this should be used to ensure action items are addressed.

6.1.3 Media Interaction - Training sessions on how to appropriately interact with the media regarding incidents and incident response can improve the team's incident response capability. Media interaction training should cover:

6.1.4 Sensitive Information - Media interaction training should include the importance of not revealing sensitive information such as confidential information, and technical details of countermeasures and response techniques.

6.1.5 Effective Communication - Media interaction training should include techniques for communicating important information consistently, fully, and effectively.

6.1.6 Handling the Media - Media interaction training should include techniques for handling interactions with the media effectively.

6.2 (P) Incident Response Team Testing and Exercises - The BU shall test the incident response capability for the state information system annually using checklist, walkthrough, tabletop exercises, simulations or comprehensive exercises to determine the incident response effectiveness and document the results.

6.2.1 **Incident Response Exercises** - The incident response team should exercise their incident response capability. The purpose of an exercise is to validate the viability of one or more aspects of the incident response plan.

a. **Exercise Type** - The BU should implement either a tabletop exercise or a functional exercise to validate the content of the incident response plan.

a. **Tabletop Exercises**: Discussion-based exercises involving incident response personnel in a classroom setting to discuss roles and responses in a particular emergency situation.

b. **Functional Exercises**: Performance-based exercises involving incident response personnel in a simulated operational environment.

6.2.2 **Exercise Elements** - The following elements should be in place to ensure an effective exercise:

a. **Determine Aspects**. An incident response exercise is designed to test one or more aspects of the incident response plan (e.g., communications, emergency notifications, IT equipment setup). The incident response team lead should determine and document which aspects of the IR plan are to be exercises and ensure that the functional exercise is designed and planned to test those aspects.

b. **Coordination**. Exercises should involve multiple BU departments and potentially other BUs to ensure that coordination aspects of the plan are exercised as well.

c. **Scenario**. An exercise shall be based on a selected and documented scenario. A scenario is a sequential, narrative account of a hypothetical incident. The scenario should be accompanied by a list of questions regarding the incident that elicits an exercise of the incident response plan.

d. **Facilitation** - An exercise facilitator should present a scenario to the assembled team, initiate discussion amongst the team by posing scenario-related response questions, and cover the topics of roles, responsibilities, coordination, and decision-making.

e. **Documentation** - A resource should be allocated to record the important aspects and results of the meeting: team's knowledge and use of existing procedures, allocation of roles and responsibilities, ability to coordinate among participants, and effectiveness of the decision-making process.

6.3 Security and Privacy Incident Response Plan Template - The following template may be used to create a state system security and/or privacy incident response plan.

6.3.1 Introduction - This is the incident response plan for the [state information system] that documents the team members, system information, and procedures for responding to a security incident.

6.3.2 System Overview - The following overview of the state information system provides the necessary background of the system to support incident response.

a. Network Diagram - [insert a current network diagram of the state information system along with a labeling and an explanation of the system components, interfaces, media of component connections, and interfaces to third party systems.]

b. Data Flow Diagram - [insert a data flow diagram of the state information system along with a labeling and an explanation of the system components, interfaces, media of component connections, and data.]

c. State Information System Hardware Inventory - [insert a hardware inventory of the state information system.]

d. State Information System Logging - [insert a description and details of the available audit logs on the system. Include a description of the contents of the logs and the location of the logs.]

6.3.3 Roles and Responsibilities - The [*state information system*] incident response (IR) team includes the following members:

[Insert a roles and responsibilities matrix – example below.]

Title	Role	Responsibilities
IR Team Lead	Leadership for the incident response team.	● Lead responsibility for the BU response to system security incidents.
Authorizing Official	State information system authority with decision-making authority in the event of a declared incident.	● Understand mission impacts in the event of system data compromise or modification, or unavailability of the system or system functions. ● Authorize actions and decisions of the incident response team.

BU Organizational Unit Representative	Represent the interest of and access to expertise within the BU organizational unit.	● Represent the BU organizational unit (OU) during responses that involve BU OU systems, mission, or personnel.
Information Security Officer	Functional responsibility for information security within the BU.	● Determines the nature and scope of the incident ● Contacts qualified information security specialists for advice as needed ● Contacts members of the Incident Response Team ● Determines which Incident Response Team members play an active role in the investigation ● Provides proper training on incident handling ● Escalates to executive management as appropriate ● Contacts auxiliary departments as appropriate ● Monitors progress of the investigation ● Ensures evidence gathering, chain of custody, and preservation is appropriate ● Prepares a written summary of the incident and corrective action taken
Director of Information Technology	Functional responsibility for BU information technology.	● Coordinates technical activities and access to technical expertise or information.
Information Privacy Officer	Functional responsibility for privacy within the BU.	● Coordinates activities with the Information Security Office ● Documents the types of personal information that may have been breached ● Provides guidance throughout the investigation on issues relating to privacy of customer and employee personal information ● Assists in developing appropriate communication to impacted parties ● Assesses the need to change privacy policies, procedures, and/or practices as a result of the breach. ● Determines privacy impact of the incident. ● Implements privacy-specific elements of the privacy incident response plan (e.g., privacy impact, breach logging, and notification).
Network Technology Lead	Lead expert for technology related activities.	● Analyzes network traffic for signs of denial of service, distributed denial of service, or other external attacks ● Runs tracing tools such as sniffers, Transmission Control Protocol (TCP) port monitors, and event loggers ● Looks for signs of a firewall breach ● Contacts external Internet service provider for assistance in handling the incident ● Takes action necessary to block traffic from suspected intruder

Title	Role	Responsibilities
Operating System Technology Lead	Lead expert for operating system related activities.	● Ensures all service packs and patches are current on mission-critical computers ● Ensures backups are in place for all critical systems ● Examines system logs of critical systems for unusual activity
Business Applications Lead	Lead expert for business application related activities.	● Monitors business applications and services for signs of attack ● Reviews audit logs of mission-critical servers for signs of suspicious activity ● Contacts the Information Technology Operations Center with any information relating to a suspected breach ● Collects pertinent information regarding the incident at the request of the Chief Information Security Office
Internal Audit	Lead expert for internal audit related activities.	● Reviews systems to ensure compliance with information security policy and controls ● Performs appropriate audit test work to ensure mission-critical systems are current with service packs and patches ● Reports any system control gaps to management for corrective action
Communications Officer	Responsibility and authority to release security incident response information to the public or external parties.	● Handles requests from media for information regarding incidents. ● Prepares and disseminated information for release regarding incidents.

Table 1. Example Incident Response Team Roles and Responsibilities. *The incident response team includes experts, functional leaders, and senior management to ensure adequate coverage of required incident response activities.*

6.3.4 Incident Response Detection and Analysis - The BU has a process in place to detect incidents, analyze the available data and respond appropriately. This process begins with detection and analysis.

a. **Identification and Classification** - Upon indication of a potential state information system incident, [insert role] identifies and classifies the incident for tracking appropriate response Table 2 below documents the incident type and classifications used.

[Insert an Incident Identification Table – example below.]

Incident Identification	Description	Examples
System Misuse	Use of state information system or associated resources or data by an authorized user in violation of established policies and procedures.	● Unauthorized access of accounts or files ● Misuse of system privileges ● Attempts to circumvent security controls

System Attack	Attempts by an unauthorized user to gain access to state information system or associated resources or data or attempts to disrupt state information system services	● Denial of service attack ● Introduction of malware ● Hacking attempts ● Spam or malicious email
Technical Vulnerabilities	A reported weakness in an existing control.	● Unencrypted confidential data detected ● Failed penetration testing results
Physical	Theft or loss of state information system components or unauthorized access to premises or confidential data.	● Loss of stolen laptop ● Loss of stolen cell phone with BU data ● Physical break-in

Table 2. Incident Identification. *Information security incidents are identified and classified according to the threat source and vulnerability area.*

b. Investigate Severity - Upon indication of a potential [state information system] incident, [insert role] identifies and classifies the incident for tracking an appropriate response. The severity of the incident is declared to ensure the application of appropriate resources. The criteria used to determine and declare the severity of each tracked incident is in Table 3, below.

[Insert an incident severity and escalation table – example below.].

Severity	Description	Examples	Escalation Level	Affected Team Members	Action Required
Low	Non-threatening incidents to BU state information systems of assets.	● Limited number of unsuccessful attempts to penetrate state information systems. ● Non-malicious behaviors that violate BU policy.	0	● Network Security Monitoring	● Monitor IDS alerts ● Gather firewall log records. ● Conduct detailed analysis.
Moderate	Potential threat to systems or confidential data indicated by an event or pattern of events.	● Patterns of repeated low severity incidents. ● Suspicious patterns of incoming data from external sources. ● Malicious email	1	● Network Security Monitoring ● Information Security Officer ● Network Operations Team	● DETERMINE DEFENSIVE ACTIONS. ● CONTINUE LOGGING ALL ACTIVITY RELATED TO THE INCIDENT.

Severity	Description	Examples	Escalation Level	Affected Team Members	Action Required
High	Confirmed threat to systems or confidential data indicated by an event of pattern of events.	- Prolonged and confirmed attack on system from external source. - Penetration or denial of service attacks resulted in limited impact on operations.	2	- Network Security Monitoring - Information Security Officer - Network Operations Team - Incident Response Team Lead - Dir. of IT	- IRT LEAD: DETERMINE COURSE OF ACTION. - IRT Coordinator: assist in informing appropriate IRT members.
	Confirmed breach of system or confidential data with limited impact.	- Limited disclosure of confidential information. - Confirmed unauthorized access of system or confidential data.	3	- Network Security Monitoring - Information Security Officer - Privacy Officer (if PII related) - Network Operations Team - Incident Response Team Lead - Dir. of IT	
Critical	Confirmed breach of system or confidential data.	Successful penetration or denial of service attacks have been detected that have a significant impact on critical operations. Significant disclosure of confidential information	4	- Network Security Monitoring - Information Security Officer - Privacy Officer (if PII related) - Network Operations Team - Incident Response Team Lead - Dir. of IT - Chief Information Officer - Human Resources (if employee related)	- CONTACT HR (IF EMPLOYEE RELATED) - CONTACT LAW ENFORCEMENT IF PURSUING LEGAL ACTION...

Table 3. Incident Severity and Escalation Levels. *Information security incidents assigned severity and escalation levels according to the intent, success, and impact of the incident.*

6.3.5 **Documentation and Evidence Preservation** - Evidence of the system security incident may be required for legal prosecution, insurance, or other reasons. To properly preserve evidence all relevant information collected during the incident handling shall be identified, protected, and preserved. Documentation of the incident may be used for forensic purposes and therefore must be properly collected and preserved. Forensic evidence collection and preservation is covered in a forensics procedures manual. Documentation collected for an incident requiring investigation must contain the following elements:

- **a.** What happened – describe the incident based on available information
- **b.** Where it happened – include location and identification information known or as presented (e.g., IP address, systems involved, physical locations)
- **c.** When it happened – include date and time in an incident time line.
- **d.** Who did it – include information on the identity of the suspect as known (e.g., account information, IP address, name of individual)
- **e.** How they did it – include methods of the incident as known

6.3.6 Forensic Evidence Collection - Evidence of the state information system security incident may be required for legal prosecution, insurance, or other reasons. To properly preserve evidence all relevant information collected during the incident handling shall be identified, protected, and preserved. Documentation of the incident used for forensic purposes must be properly collected and preserved. Forensic evidence collection and preservation is covered in more detail in a forensics procedures manual. The basics of the evidentiary chain are outlined below:

- **a. Evidence Collection** - Record when, where, and who discovered the evidence. Information from the incident response or ticketing form shall match. Additional information is added as known.
- **b. Evidence Handling** - Record who has handled or examined the evidence and when it was handled.
- **c. Evidence Custody** - Record who has had custody of the evidence, during what time period, where it has been stored, and how it has been secured. Any change in custody must also be documented.

6.3.7 Forensic Evidence Storage - All information related to an incident investigation shall be stored securely. Access to this information shall be limited to authorized personnel (e.g., incident response team, management, legal team). If evidence is transferred to another party (e.g., law enforcement) an itemized inventory of all evidence shall be created and retained by the BU.

6.3.8 Incident Communication - The control of information regarding any suspected or confirmed system security incident is critical to the protection of the BU mission, our ability to respond appropriately to the incident, and to the protection of confidential information. Unauthorized personnel may not discuss or release any information regarding a system security incident. Incident communication is limited to authorized personnel. State information security incident data and reports are classified as confidential information and may only be downgraded (to public) by the authorized Communications Officer.

a. In the event that the incident is determined to be a breach involving PII, the BU Privacy Officer will determine the need for and manner in which a breach notification is handled. The BU Breach Notification Process will dictate the necessary steps (see P8420 Incident Response Policy 6.9.2 Notification.)

6.3.9 Incident Response Containment, Eradication and Post Incident Checklist - [Each BU will need to determine the most appropriate response strategy based on their systems, data, threats, mission, and capability. The following checklist/outline of the incident response, containment, eradication and post incident process should be modified and expanded to meet the BU needs.]

DETECTION AND ANALYSIS		**COMPLETED**
1	Identify incident based on threat source and vulnerability area.	
2	Prioritize the incident based on the severity and escalation level.	
3	Identify which systems, system components, and data have been affected and forecast additional assets that may be affected.	
4	Estimate the current and potential technical effect of the incident.	
5	Report the incident to the Chief Information Officer and appropriate personnel organizations.	
CONTAINMENT, ERADICATION AND RECOVERY		**COMPLETED**
6	Stop or try to contain the incident if it is still in progress.	

	Disconnect affected systems from the network.	
7	Preserve evidence from the incident. Make copies of the log files that contain evidence related to the incident if possible.	
8	Wipe out all effects of the incident. If a system has been compromised, rebuild it from known trusted sources.	
9	Identify and mitigate all vulnerabilities that were exploited.	
10	Remove malicious code, inappropriate materials and other components.	
11	Recover from the incident.	
12	Return affected systems to an operationally ready state.	
13	Confirm that the affected systems are functioning normally.	
14	If necessary, implement additional monitoring to look for future related activity.	
POST-INCIDENT ACTIVITY		**COMPLETED**
15	Create follow-up report (after action report).	
16	Hold a lesson-learned meeting.	
17	Estimate damage/impact.	
18	Review what actions were taken during the incident.	
19	Make changes to the policies and procedures if necessary.	

Appendix A: Contact List

Title	Contact Name	Phone Numbers
IR Team Lead		
Authorizing Official		
BU Organizational Unit Representative		
Information Security Officer		
Director of Information Technology		
Information Privacy Officer		

Network Technology Lead		
Operating System Technology Lead		

Title	Contact Name	Phone Numbers
Business Applications Lead		
Internal Audit		
Communications Officer		
Law Enforcement Contact		
(P) Payment Brand Contact		

7. DEFINITIONS AND ABBREVIATIONS

7.1 Event any observable occurrence in the system.

7.2 Adverse Event events with a negative consequence such as a system crashes, unauthorized access, or introduction of malware.

7.3 Security Incident a violation or imminent threat of violation of state system security policies.

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

8. REFERENCES

8.1 NIST 800-61 Rev. 2, Computer Security Incident Handling Guide, August 2012.

8.2 NIST 800-84, Guide to Test, Training, and Exercise Program for IT Plans and Capabilities, September 2006.

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

9. ATTACHMENTS

None.

10. REVISION HISTORY

Date	Change	Revision	Signature
01/01/2014	Initial Release	DRAFT	Aaron Sandeen, State CIO and Deputy Director
5/26/21	Annual Updates	3.0	Tim Roemer, Director of Arizona Department of Homeland Security & State Chief Information Security Officer Tim Roemer Tim Roemer (May 25, 2021 22:11 PDT)