COMPLIANCE COMPONENT

DEFINITION	
Name	Incident Response Policies, Procedures and Training

Description	Incident Response Policies and Procedures help communicate to the State's IT community and interested parties (external agencies and the public) about discovered security threats and breaches. Policies and Procedures should help agencies record and document the following:
	• Contact information for the recipient of the incident response report;
	• Incident description;
	  ○ Date, Time, and location where the incident occurred
	  ○ How the incident was discovered
	  ○ IP Address/Host Name/Physical location of the breach
	  ○ What data was compromised
	  ▪ Type or types of data compromised
	  ▪ Sensitivity of data/parties affected
	  ○ Actions taken to mitigate the damages
	  ○ Other parties contacted regarding the incident
	• Contact information for the person reporting the incident
	  ○ Name, title and signature of the reporting official
	• Time and Date incident was resolved (if applicable)
	• Method of incident resolution
	Incident Response Training teaches state employees about their responsibilities in the event of a security incident.

Rationale	Agencies handling confidential information need to have policies and procedures in place to assist them when responding to security incidents. Incident response training is associated with the assigned roles and responsibilities of organizational personnel to ensure that the appropriate content and level of detail are included in such training.
Benefits	• Provides responders with a comprehensive and structured response to a security incident. • Helps to minimize the damage from security incidents • Builds knowledge base

ASSOCIATED ARCHITECTURE LEVELS	
Specify the Domain Name	Security
Specify the Discipline Name	Operational Controls
Specify the Technology Area Name	Incident Response
Specify the Product Component Name	

COMPLIANCE COMPONENT TYPE	
Document the Compliance Component Type	Guideline
Component Sub-type	

COMPLIANCE DETAIL

State the Guideline, Standard or Legislation	**Policies and Procedures** a. Develop, document, and disseminate to agencies: 1. An incident response policy that: i. Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and ii. Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and 2. Procedures to facilitate the implementation of the incident response policy and the associated incident response controls; i. Designate a point of contact to manage the development, documentation, and dissemination of the incident response policy and procedures; and ii. Review and update the current incident response: 1. Policy annually and following a major security incident; and 2. Procedures annually and following a major security incident. **Training** a. Provide incident response training to system users consistent with assigned roles and responsibilities: 1. During the onboarding process of assuming an incident response role or responsibility or acquiring system access; 2. When required by system changes; and 3. Annually thereafter; and b. Review and update incident response training content annually and following a major security incident.
Document Source Reference #	NIST 800-53 rev. 5, NIST SP 800-61 rev. 2

Compliance Sources

Name	National Institute of Standards and Technology (NIST))	*Website*	http://csrc.nist.gov/
Contact Information	inquiries@nist.gov		
Name		*Website*	
Contact Information			

KEYWORDS

List Keywords	Intrusion detection, exposure, vulnerability, attack, incident, threat, risk, alerts, communication, denial of service, breach.

COMPONENT CLASSIFICATION

Provide the Classification	☐ *Emerging*	☒ *Current*	☐ *Twilight*	☐ *Sunset*
Sunset Date				

COMPONENT SUB-CLASSIFICATION

Sub-Classification	Date	Additional Sub-Classification Information
☐ *Technology Watch*		
☐ *Variance*		

☐ *Conditional Use*		

Rationale for Component Classification	
Document the Rationale for Component Classification	

Migration Strategy	
Document the Migration Strategy	

Impact Position Statement	
Document the Position Statement on Impact	

CURRENT STATUS				
Provide the Current Status	☐ *In Development*	☐ *Under Review*	☒ *Approved*	☐ *Rejected*

AUDIT TRAIL			
Creation Date	12/19/2002	*Date Approved / Rejected*	06/13/2023
Reason for Rejection			
Last Date Reviewed	06/07/2023	*Last Date Updated*	06/13/2023
Reason for Update	Vitality		