COMPLIANCE COMPONENT

DEFINITION	
Name	Incident Response Reporting

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

Rationale	Agencies handling confidential information need to have plans and procedures in place to assist them when responding to security incidents.
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	State of Missouri Incident Response Plan and Procedures
Document Source Reference #	NIST 800-53 rev 4, 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	Currently the active plan and procedures authorized by Information Technology Advisory Board.

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*	01/21/2003
Reason for Rejection			
Last Date Reviewed		*Last Date Updated*	12/12/2017
Reason for Update	Vitality		