



Compliance Component

DEFINITION

<i>Name</i>	Incident Response Reporting
<i>Description</i>	<p>Plan and procedures to help ensure the State's IT community is aware of information security threats and concerns. Plan and Procedures should record and document the following:</p> <ul style="list-style-type: none"> ❑ Attempts (failed or successful) to gain unauthorized access to systems or data; ❑ Unwanted disruption or denial of service; ❑ The unauthorized use of a system for the transmission, processing or storage of data; ❑ Changes to system hardware, firmware, or software characteristics without the owner's knowledge, instruction or consent.
<i>Rationale</i>	Minimizes the damage from security incidents and facilitates communication throughout State agencies.
<i>Benefits</i>	Promotes awareness of incidents; allows for monitoring; builds knowledge base – collecting the right information enables the creation of useful reports (big picture/patterns); standardization

ASSOCIATED ARCHITECTURE LEVELS

<i>List the Domain Name</i>	Security
<i>List the Discipline Name</i>	Operational Controls
<i>List the Technology Area Name</i>	Incident Response
<i>List the Product Component Name</i>	

COMPLIANCE COMPONENT TYPE

<i>Document the Compliance Component Type</i>	Guideline
<i>Component Sub-type</i>	

COMPLIANCE DETAIL

<i>State the Guideline, Standard or Legislation</i>	State of Missouri Incident Response Plan and Procedures
<i>Document Source Reference #</i>	http://www.oa.state.mo.us/dis/tech_services/incident.htm

Standard Organization

<i>Name</i>	OA Information Security Management Office (ISMO)	<i>Website</i>	http://www.oa.state.mo.us/dis/tech_services/security.htm
<i>Contact Information</i>	Division of Information Services Room 280, 301 W. High Jefferson City, MO 65101 573.751.3290		

Government Body			
<i>Name</i>	Information Technology Advisory Board (ITAB)	<i>Website</i>	http://www.oit.state.mo.us/itab/itab.html
<i>Contact Information</i>	Security Committee		
KEYWORDS			
<i>List all Keywords</i>	INFOCON; intrusion detection; exposure; vulnerability; attack; incident impacts; defense; threat; risk; alerts; communication; denial of service		
COMPONENT CLASSIFICATION			
<i>Provide the Classification</i>	<input type="checkbox"/> <i>Emerging</i> <input checked="" type="checkbox"/> <i>Current</i> <input type="checkbox"/> <i>Twilight</i> <input type="checkbox"/> <i>Sunset</i>		
Rationale for Component Classification			
<i>Document the Rationale for Component Classification</i>	Currently the active plan and procedures authorized by Information Technology Advisory Board.		
Conditional Use Restrictions			
<i>Document the Conditional Use Restrictions</i>			
Migration Strategy			
<i>Document the Migration Strategy</i>			
Impact Position Statement			
<i>Document the Position Statement on Impact</i>			
CURRENT STATUS			
<i>Provide the Current Status</i>	<input type="checkbox"/> <i>In Development</i> <input type="checkbox"/> <i>Under Review</i> <input checked="" type="checkbox"/> <i>Approved</i> <input type="checkbox"/> <i>Rejected</i>		
AUDIT TRAIL			
<i>Creation Date</i>	12-19-2002	<i>Date Accepted / Rejected</i>	01-21-2003
<i>Reason for Rejection</i>			
<i>Last Date Reviewed</i>		<i>Last Date Updated</i>	
<i>Reason for Update</i>			