Tier 1 Control Standards (State-Wide)

Incident Response Team

Standard ID
IOT-CS-SEC-133

Published Date
3/16/2006

Effective Date
3/16/2006

Last Updated
5/19/2017

Next Review Date
5/19/2018

Policy
16.0 Communications (RS.CO)
16.4 RS.CO-4
16.4.1 Response Plan Coordination

Purpose
This Standard identifies the Information Security Incident Response Team (ISIRT) and supports the effective handling of security incidents.

Scope
IOT Supported Entities

Statement
A number of information security incidents will affect the state each year. To help agencies respond effectively to incidents, a team has been organized with skills and experience capable of assisting agencies through the difficult process of dealing with a security breach. The State’s ISIRT is to be engaged by agencies regardless of the size or scope of an incident. Involvement of the team and of individual team members will vary depending on the nature of the event.

Below are the requirements for incident response:
- Agencies shall consult their incident management procedures as developed per direction provided in the Incident Planning and Management Standard.
- Agencies shall engage the ISIRT for assistance by direct phone call to the CIO or CISO. Upon discussion of the factors involved, the agency and IOT leadership shall determine the individual that assumes the role of “incident manager”.
- The CIO, CISO or their designee shall engage other members of the ISIRT as needed, and other resources as necessary (technical roles such as DBA, OS admins, etc.), and follow-up with the agency regarding the incident.
- The ISIRT (a portion or all depending on the circumstances) will meet with the agency to discuss appropriate next steps.
- The agency, engaging the ISIRT team as needed, will manage incidents involving less than 500 records through conclusion. For incidents over 500 records, the ISIRT team and agency will co-manage the incident through resolution.
- The agency and CISO will put in necessary measures to inhibit a recurrence of the incident both at an agency and statewide level.
- The CISO documents the incident for future risk mitigation activities at an enterprise level.

Roles
Agency Executive Management
IOT Personnel
Responsibilities
Agency Management/Executive Management must be aware of and be able to execute the requirements written within this Standard for Incident Response. IOT shall maintain the ISIRT and work with agencies in accordance with this Standard.

Management Commitment
Management is responsible for ensuring their agency is meeting the requirements written within this standard.

Coordination Among Organizational Entities
Agencies shall coordinate with IOT when an incident has occurred or may have occurred.

Compliance
Failure to report incidents to the ISIRT may result in disciplinary action.

Exceptions
No exceptions.