

	Department of Administration Policy	Category	Incident Response, SITSD Security
		Effective Date	04/01/2009
		Last Revised	01/15/2014
Issuing Authority	State Information Technology Services Division		
POL-Incident Response Policy			

I. Purpose

The purpose of this Policy is to establish the requirement for the State Information Technology Services Division (SITSD) to implement Incident Response for information systems that SITSD manages or controls.

II. Scope

This Policy encompasses information systems that SITSD manages or controls, including systems that third-parties manage or host on SITSD's behalf.

III. Policy Statement

SITSD shall develop and implement Incident Response for the state's enterprise information systems maintained by SITSD based on the [National Institute of Standards and Technology \(NST\) SP800-53 Revision 4 Security and Privacy Controls for Federal Information Systems and Organizations](#), and associated NIST guidelines and standards.

IV. Roles and Responsibilities

The following roles and responsibilities are required by this policy:

- A. Chief Information Officer:** Oversees the information technology resources that maintain information systems for SITSD.
- B. Chief Information Security Officer:** Ensures compliance with security policies and procedures within SITSD.
- C. Chief Technology Officer:** Monitors organization compliance and may make enforcement recommendations to the appropriate level of management given the particular circumstances.

- D. Chief Intergovernmental Relations Officer:** Monitors organization compliance and may make enforcement recommendations to the appropriate level of management given the particular circumstances.
- E. Chief Operations Officer:** Monitors organization compliance and may make enforcement recommendations to the appropriate level of management given the particular circumstances.
- F. Chief Financial Officer:** Monitors organization compliance and may make enforcement recommendations to the appropriate level of management given the particular circumstances.
- G. Division Personnel:** Responsible for implementation of requirements that are contained in policies and procedures.

V. Requirements

To support Incident Response, this Policy requires that SITSD shall:

1. Implement this Policy in compliance and integrated with guidance provided by the [National Institute of Standards and Technology Guidance](#). Specific requirements for SITSD include:
 - a. Allocation of adequate resources to respond quickly and effectively when an incident occurs.
 - b. Implement the Information Systems Incident Response Team (ISIRT) for each declared incident.
 - c. Incorporate incident response training in its overall employee training program.
 - d. Implement a testing plan for incident response that will be activated on a bi- basis.
 - e. Have an incident response support resource through the Information Systems Security Office (ISSO) that offers support for mitigation and reporting of incidents.
2. Establish procedures and associated supporting documents to support the incident response process.
3. Establish and evaluate performance measures to assess implementation of this Policy, procedures, and associated documents.
4. Annually review the incident response policy, procedure(s), and associated documents and make any necessary changes to provide efficient and effective response to information system incidents.

VI. Definitions

Refer to the [NIST Information Security Glossary of Key Information Security Terms](#) for a list of NIST definitions.

VII. Compliance

Compliance shall be evidenced by implementing the Incident Response Policy as described above.

VIII. Enforcement

Each bureau is responsible for the Policy's implementation and enforcement. The Chief Technology Officer, Chief Business Officer, and Chief Operations Officer shall monitor bureau compliance and may make enforcement recommendations to the appropriate level of management given the particular circumstances.

If warranted, management shall take appropriate disciplinary action to enforce this Policy, up to and including termination of employment, consistent with current State Policy. The discipline policy can be found in the [MOM Policy System](#) (*search for: 261*). When considering formal disciplinary action, management will consult with their assigned Human Resource Specialist before taking action.

IX. References

A. Legislation

- [2-15-112 MCA](#) - Duties and Powers of Department Heads

B. Policies, Directives, Regulations, Rules, Procedures, Memoranda

- SITSD Procedure: [PRO-IT Policies, Standards, Procedures and White Papers Procedure](#)

C. Standards, Guidelines

- [NIST SP800-53 Revision 4 Security and Privacy Controls for Federal Information Systems and Organizations](#)