

	Department of Administration Policy	Category	Planning, SITSD Security
		Effective Date	12/01/2010
		Last Revised	02/27/2015
Issuing Authority	State Information Technology Services Division		
POL-Security Planning Policy			

I. Purpose

The purpose of this Policy is to establish the requirement for the State Information Technology Services Division (SITSD) to implement Security Planning 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 Security Planning 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 Security Planning, 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](#).
Security Planning is a key component to having a successful information security program. Specific requirements for SITSD include:
 - a. Developing and maintaining an overall information system security plan.
 - b. Developing, documenting, periodically updating, and implementing security plans for information systems that describe the security controls in place or planned for the information systems and the rules of behavior for individuals accessing the information systems.
 - c. The use of the SITSD planning template to document the security plans for information systems.
 - d. The authorization of information system security plans.
 - e. Reviewing and updating of information security plans when significant changes have occurred in the system or security requirements have changed.
 - f. Planning and coordinating security related activities affecting information systems before conducting such activities. This will be accomplished through the change management process.

2. Establish procedures and associated supporting documents to support the security planning process.
3. Allocate adequate resources to support the security planning process.
4. Establish and evaluate performance measures to assess implementation of this Policy, procedures, and associated documents.
5. Annually review the security planning policy, procedure(s), and associated documents and make any necessary changes to provide adequate support for the security planning process.

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 Security Planning 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](#)