

	Department of Administration Policy	Category	Media Protection, SITSD Security
		Effective Date	05/01/2010
		Last Revised	03/31/2014
Issuing Authority	State Information Technology Services Division		
POL-Media Protection Policy			

I. Purpose

The purpose of this Policy is to establish the requirement for the State Information Technology Services Division (SITSD) to implement Media Protection 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 Media Protection 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. Requirements

To support Media Protection, 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](#).

Media Protection is an important aspect of an overall security program. Specific requirements for SITSD include:

- a. Restricting access to information system media to authorized individuals.

- b. Labeling of removable information system media and output indicating distribution limitations, handling caveats, and applicable security markings.
 - c. Applying of physical security controls and securely storing information system media within controlled areas.
 - d. Protecting and controlling information system media during transport outside of controlled areas and restricting the activities associated with transport of such media to authorized personnel.
 - e. Sanitizing information system media, both digital and non-digital, prior to disposal or release for reuse.
2. SITSD shall establish procedures and associated supporting documents to support an information system media protection program.
 3. SITSD shall allocate adequate resources to support a media protection program.
 4. SITSD shall establish and evaluate performance measures to assess implementation of this Policy and associated procedures.
 5. SITSD shall review the media protection procedure(s), and associated documents on an annual basis and make any necessary changes to them.

V. 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.

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 Media Protection 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](#)