

| | | | |
|---|--|----------------|--|
|  | Department of Administration Policy | Category | SITSD Security, System and Information integrity |
| | | Effective Date | 02/01/2010 |
| | | Last Revised | 02/03/2015 |
| Issuing Authority | State Information Technology Services Division | | |
| POL-System and Information Integrity Policy | | | |

I. Purpose

The purpose of this Policy is to establish the requirement for the State Information Technology Services Division (SITSD) to implement System and Information Integrity 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 System and Information Integrity for the state's enterprise information systems maintained by SITSD based on the [National Institute of Standards and Technology \(NIST\) 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 System and Information Integrity, 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](#).
Protection of the integrity of systems and information is a key component to having a stable information systems environment. Specific requirements for SITSD include:
 - a. Identifying, reporting, and correcting information system flaws through a patch management program.
 - b. Implementing malicious code protection at critical information system entry and exit points and at workstations, servers, or mobile computing devices on the network.
 - c. Monitoring of events that detect attacks and provide identification of unauthorized use of information systems.
 - d. Receiving security alerts/advisories on a regular basis, issuing alerts/advisories to appropriate personnel, and taking appropriate actions in response to alerts/advisories.
 - e. Applying verification processes for integrity of software and information.

- f. Implementing spam protection.
 - g. Checking information for accuracy, completeness, validity, and authenticity.
 - h. Identifying and handling error conditions in an expeditious manner without providing information that could be exploited by adversaries. [Errors are sent only to designated individuals and the information sent does not contain sensitive data such as Social Security Numbers, account numbers, etc.](#)
 - i. Applying Federal Desktop Configuration Standards to employee desktop computers. [This would include the disallowance of tethering non-state owned devices to the desktop or laptop computer.](#)
2. Establish procedures and associated supporting documents to support the protection of the integrity of systems and information.
 3. Allocate adequate resources to protect the integrity of systems and information.
 4. Establish and evaluate performance measures to assess implementation of this Policy, procedures, and associated documents.
 5. Review the System and Information Integrity Policy, procedure(s), and associated documents on an annual basis and make any necessary changes to provide adequate support to protect the integrity of systems and information.

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 System and Information Integrity 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

- Statewide Policy: [Computer Security Incident Management](#) (*search for: 323*)
- 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](#)