

	<b>Department of Administration</b>  <b>Policy</b>	Category	<b>Audit and Accountability, SITSD Security</b>
		Effective Date	<b>03/01/2010</b>
		Last Revised	<b>06/27/2014</b>
Issuing Authority	<b>State Information Technology Services Division</b>		
<b>POL-Audit and Accountability Policy</b>			

### **I. Purpose**

The purpose of this Policy is to establish the requirement for the State Information Technology Services Division (SITSD) to implement Audit and Accountability 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 Audit and Accountability 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 Audit and Accountability, 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](#).

Auditing of information systems provides accountability for system and configuration changes or other actions taken by employees to modify information systems. The Auditing and Accountability process is defined to review information systems for consistency and ensure that policies and procedures are being followed appropriately.

Specific requirements for SITSD include:

- a. Generating audit records for events determined through the risk assessment process.
- b. Producing audit records that contain sufficient information to establish what events occurred, the source of the events, the outcome of the events and the date and time at which they occurred.
- c. Allocating sufficient audit record storage capacity and implementing a notification system to alert administrators of when the storage is near its capacity.
- d. Implementing an alert mechanism to contact appropriate staff in the event of an audit processing failure and documenting actions to be taken to correct the failure.
- e. Protecting audit information and tools from unauthorized access, modification, and deletion.

2. Review audit records on a monthly basis. Any inappropriate or unusual activities will be noted and the incident response process will be followed, if necessary.
3. Review information system accounts for both individual and group access on an annual basis.
4. Review firewall access on an annual basis to ensure that least privilege is being followed.
5. Conduct quarterly scans for unauthorized wireless access points.
6. Review physical access configurations to SITSD facilities on an annual basis to ensure Policy and procedure compliance. Visitor access records will be included in this review.
7. Review the Audit and Accountability program, procedure(s), and associated documents on an annual basis. Necessary changes will be made as needed to support on-going processes.

## **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 Audit and Accountability 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](#)