

	<b>Department of Administration</b>  <b>Policy</b>	Category	<b>Personnel Security, SITSD Security</b>
		Effective Date	<b>05/01/2010</b>
		Last Revised	<b>02/26/2015</b>
Issuing Authority	<b>State Information Technology Services Division</b>		
<b>POL-Personnel Security Policy</b>			

### I. Purpose

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

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

- a. Assigning risk designations to all positions and establishing screening criteria, including background checks, for individuals filling those positions within SITSD.
- b. Screening of individuals requiring access to information systems prior to authorizing access.
- c. Upon termination of individual employment, terminating information system access, conducting exit interviews, retrieving all information system-related property, and providing appropriate personnel with access to official records created by the terminated employee that are stored on information systems.
- d. Reviewing information system/facilities access authorizations when personnel are reassigned or transferred to other positions within SITSD.
- e. Requiring appropriate access agreements for individuals requiring access to information systems before authorizing access.
- f. Establishing and monitoring personnel security requirements for third-party providers.

- g. Employing a formalized sanction process for personnel failing to comply with established information security policies and procedures.
2. SITSD shall establish procedures and associated supporting documents to support an information system personnel security program.
3. SITSD shall allocate adequate resources to support a personnel security program.
4. SITSD shall establish and evaluate performance measures to assess implementation of this Policy and associated procedures.
5. SITSD shall review the personnel security procedure(s), and associated documents on an annual basis and make any necessary changes to them.

## **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 Personnel Security 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](#)