

	Department of Administration Policy	Category	Awareness and Training, SITSD Security
		Effective Date	12/01/2009
		Last Revised	08/11/2014
Issuing Authority	State Information Technology Services Division		
POL-Awareness, Training, and Education Policy			

I. Purpose

The purpose of this Policy is to establish the requirement for the State Information Technology Services Division (SITSD) to implement Awareness, Training, and Education 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 Awareness, Training, and Education 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 Awareness, Training, and Education, 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 Awareness, Training, and Education are key components to having a successful information security program. Specific requirements for SITSD include:
 - a. Designing, developing, implementing, and updating an overall security awareness and training program for SITSD.
 - b. Providing basic security awareness training to all new information system users within SITSD.
 - c. Providing refresher security awareness training to all information system users within SITSD on an annual basis.
 - d. Providing security training for all major systems before access is allowed so that information system users understand their security responsibilities for that particular system.
 - e. Documenting security awareness training records including the listing of attendees.

- f. Providing annual promotional events during Cyber Security Awareness Month.
2. Establish procedures and associated supporting documents to support the security awareness, training, and education process.
3. Allocate adequate resources to support the security awareness, training, and education program.
4. Establish and evaluate performance measures to assess implementation, effectiveness, and efficiency of this Policy, procedures, and associated documents.
5. Review the security awareness, training, and education Policy, procedure(s), and associated documents on an annual basis and make any necessary changes to provide adequate support for the security awareness and training program.

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 Awareness, Training, and Education 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](#)