

	Department of Administration Policy	Category	SITSD Security, System and Communication Protection
		Effective Date	01/01/2010
		Last Revised	11/15/2009
Issuing Authority	State Information Technology Services Division		
POL-System and Communication Protection 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 Communication 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 System and Communication Protection security controls 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. Requirements

To support System and Communication 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](#).

Protection of information assets and communication mechanisms are key components to having a stable information systems environment. Specific requirements for SITSD include:

- a. Monitoring, controlling, and protecting communications (i.e., information transmitted or received by information systems) at the external boundaries and key internal boundaries of the information systems. This includes but is not limited to the following:
 - i. Blocking of malicious and other web sites and IP addresses at the external firewall. This would include an automatic failover mechanism when there is an operational failure of the protection device(s).
 - ii. Removing compromised systems from the network.
 - iii. Providing separation of duties in the management of communications equipment and minimizing the number of staff with administrative access to firewalls, routers, switches, etc.
 - iv. Managing network equipment utilizing a trusted communications path.
 - v. Denying all inbound and outbound network traffic with exceptions.
 - vi. Monitoring intrusion detection and other monitoring systems on a daily basis to detect and mitigate security issues.
 - vii. Protection from Denial of Service Attacks.
 - viii. Maintaining security standards for wireless networks by authorizing, monitoring, and controlling its use.
 - ix. Maintaining security standards for voice over IP systems by authorizing, monitoring, and controlling its use.
- b. Employing architectural designs, software development techniques, and systems engineering principles that promote effective information security within information systems. This includes but is not limited to the following:
 - i. Preventing public access into the internal network except as appropriately mitigated.
 - ii. Maintaining a protective environment for web and other public services needing access to protected information including, but not limited to maintaining a DMZ (Demilitarized Zone). This would limit all public access to devices located in the DMZ. This

would also include an automatic failover mechanism when there is an operational failure of the protection device(s).

- iii. Encrypting sensitive information utilizing 128-bit encryption at a minimum.
 - iv. Prioritizing resources on the network.
 - v. Isolating high priority systems on the network utilizing firewall technology or other isolation techniques.
 - vi. Maintaining and controlling the Domain Name Services (DNS) and DHCP.
 - vii. Limiting protocols used on the network to only those that are needed.
 - viii. Using private IP addressing on the internal network with translation to public networks to protect internal devices.
- c. Terminating device connections after 21 days of inactivity.
2. Establish procedures and associated supporting documents to support the protection of information systems and communications.
 3. Allocate adequate resources to protect information systems and communications.
 4. Establish and evaluate performance measures to assess implementation of this Policy, procedures, and associated documents.
 5. Review the information systems and communications protection Policy, procedure(s), and associated documents on an annual basis and make any necessary changes to provide adequate support to protect information systems and communications.

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 System and Communication 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. 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: IT Policies, Standards, Procedures and White Papers](#)

C. Standards, Guidelines

- [NIST SP800-53 Revision 4 Security and Privacy Controls for Federal Information Systems and Organizations](#)