

	Montana Operations Manual Policy	Category	Information Technology, Risk Management
		Effective Date	10/02/2013
		Last Revised	10/09/2013
Issuing Authority	Department of Administration State Information Technology Services Division		
POL-Information Technology Security Risk Management Policy			

I. Purpose

This Policy outlines the requirements for information technology security risk management.

II. Scope

This Policy applies to all executive branch agencies and independent contractors, excluding the university system, who have access to, use, or manage state government-controlled information systems.

III. Policy Statement

A. General

Agencies shall use the National Institute of Standards and Technology (NIST) publications as guidance in information technology security risk management.

B. Security Risk Management Programs

Agencies shall construct and maintain information technology security risk management programs using the NIST Special Publication 800-39 framework and Federal Information Processing Standards Publications 199 and 200 as guidance.

C. Risk Management Control Set

The state has established guidance with respect to baseline security controls, which are consistent with NIST Moderate systems. These controls are located in [Appendix A - Baseline Security Controls](#) – State of Montana. Agencies may implement additional controls beyond listed controls. Agencies will evaluate and categorize information systems as part of their respective information security management programs to determine appropriate baseline controls based on the criticality and sensitivity of the information managed by each system. Baseline controls should be evaluated as part of a risk-based security process and tailored

appropriately to achieve cost-effective, risk-based security that supports agency mission/business needs.

D. Roles and Responsibilities

[Appendix B - Security Roles and Responsibilities](#) is provided as a guide for the roles and responsibilities structure recommended for State of Montana Information Security Program management. At a minimum each department head is responsible for ensuring an adequate level of security for all data within that department and shall designate an Information Security Manager (ISM) to administer the department's security program for data (MCA 2-15-114, Security responsibilities of departments for data).

IV. References

A. Legislation

- [2-15-112 MCA Duties and Powers of Department Heads](#)
- [2-17-534, MCA – Security Responsibilities of Department](#)

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](#)

V. Contact

All inquiries regarding this document and its contents may be sent to DOASITSDRiskMgt@mt.gov.