

	Montana Operations Manual <i>POLICY TEMPLATE</i>	Category	Security
		Effective Date	
		Last Revised	
Issuing Authority	Department of Administration State Information Technology Services Division		
POL–Detect Capabilities Policy			

I. Purpose

The Montana Information Technology Act (MITA) assigns the responsibility of establishing and enforcing statewide IT policies and standards to the Department of Administration (DOA). The purpose of this Policy is to implement the (Detect Responsibilities) for defining actions to fulfill the responsibility. The POL-Detect Capabilities Policy serves to develop and implement the appropriate activities (including effective planning), to detect anomalous activity in a timely manner and understand the potential impact of events.

II. Scope

This Policy applies to the CIO as required under [2-17-521\(4\), MCA](#), and to executive branch agencies, excluding the university system, as required under Section [2-17-524\(3\), MCA](#).

III. Policy Statement

This policy has been developed for the state’s enterprise information systems maintained by DOA based on the Montana Information Technology Act (MITA). This policy is in cooperation with the federal and local governments with the objective of providing seamless access to information and services to the greatest degree possible [2-17-505 \(3\)](#).

IV. Roles and Responsibilities

Roles and responsibilities are required by this policy and in accordance with [Appendix B - Security Roles and Responsibilities](#).

V. Requirements

All agencies, staff and all others, including outsourced third-parties (such as contractors, or other service providers), who have access to, or use or manage

information assets subject to the policy and standard provisions of §2-17-534, MCA shall:

- A.** Develop, identify, and manage a baseline of normal operations and procedures for each major information system that:
 1. Establishes a documented, formally reviewed, and agreed-upon set of specifications for the information system or configuration items within the system; and
 2. Conducts configuration reviews on a bi-annual basis or as needed based on changes to the environment of operations.
- B.** Implement network and information system monitoring that:
 1. Employs automated tools to support near real-time analysis of events, with SITSD providing daily review of the audit logs during the workweek;
 2. Monitors inbound and outbound communications for unusual or unauthorized activities or conditions, (SITSD will notify agencies within 24 hours when their portion of the network is involved in any breaches of network security);
 3. Provides near real-time alerts when the following indications of compromise or potential occur:
 - account privilege escalation,
 - authentication,
 - antivirus/antimalware software,
 - user changes,
 - log errors,
 - system failures,
 - and other network failures;
 4. Monitors events in accordance with security incident and event monitoring objectives;
 5. Identifies unauthorized use of information systems;
 6. Deploys monitoring devices to strategically collect organization-determined essential information and at ad hoc locations, to track specific types of transactions of interest to the state;
 7. Heightens the level of monitoring activity whenever there is an indication of increased risk to operations and assets, individuals, other organizations, or the State based on law enforcement information, intelligence information, or other credible sources of information;
 8. Incorporates legal opinion with regard to monitoring activities in accordance with applicable federal and state laws, Executive Orders,

directives, policies, or regulations. NOTE: There are no expectations of privacy when using state computing resources unless specifically indicated by law.

- C. Conduct monitoring of physical access to information systems that:
 - 1. Includes review of physical access logs monthly; and
 - 2. Employs real-time physical intrusion alarms and surveillance equipment.
- D. Establish a continuous monitoring strategy and conduct continuous monitoring of information systems that:
 - 1. Provides information regarding current gaps in security to appropriate management officials as result of this process;
 - 2. Defines roles and responsibilities for detection to ensure accountability;
 - 3. Ensures detection activities comply with all applicable requirements;
 - 4. Ensures detection activities are tested;
 - 5. Reviews audit records on a monthly basis unless otherwise specified in the audit procedures;
 - 6. Adjusts reviews as needed depending upon the identification of possible attacks or pain points within information systems;
 - 7. Generates reports to identify suspicious activity;
 - 8. Correlates across different repositories to gain organization-wide situational awareness; and
 - 9. Continuously improves detection processes.

VI. Definitions

Refer to the [Statewide Information System Policies and Standards Glossary](#) for a list of local definitions.

VII. Compliance

Compliance shall be evidenced by implementing the Policy as described above.

Policy changes or exceptions are governed by the Procedure for Establishing and Implementing Statewide Information Technology Policies and Standards. Requests for a review or change to this instrument are made by submitting an [Action Request form](#). Requests for exceptions are made by submitting an [Exception Request form](#). Changes to policies and standards will be prioritized and acted upon based on impact and need.

VIII. Enforcement

Policies and standards not developed in accordance with this policy will not be approved as statewide IT policies or standards.

Enforcement for statewide policies and standards developed in accordance with this policy will be defined in each policy, standard or procedure.

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](#) Powers and duties of department
- [2-17-505 MCA](#) Policy
- [2-17-512 MCA](#) Duties and Powers of Department Heads
- [2-6-206 MCA](#) Protection and storage of essential records
- [2-17-524 MCA](#) Agency information technology plans – form and content – performance reports.
- [Montana Information Technology Act \(MITA\)](#)

B. Policies, Directives, Regulations, Rules, Procedures, Memoranda

- [SITSD Procedure: IT Policies, Standards, Procedures and White Papers](#)
- [Statewide Policy: Establishing and Implementing Statewide Information Technology Policies and Standards](#)