

	Montana Operations Manual <i>POLICY TEMPLATE</i>	Category	Security
		Effective Date	
		Last Revised	
Issuing Authority	Department of Administration State Information Technology Services Division		
POL–Respond 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 (Respond Capabilities Policy) for defining actions to fulfill the responsibility. The POL-Respond Capabilities Policy serves to develop and implement the appropriate activities (including effective planning), to take action regarding a cybersecurity event.

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, document, and disseminate an incident response process that:
 - 1. Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance;
 - 2. Establishes reviews and updates to incident response policy and procedures within two years of last review; and
 - 3. Incident response will follow the National Incident Management System (NIMS).
- B.** Conduct training of personnel in their incident response roles and responsibilities on an annual basis.
- C.** Conduct tests and/or exercises of the incident response capability annually using designed tabletop and real-life scenarios/exercises to determine the incident response effectiveness and documents the results. These tests may be coordinated with other groups or plans such as Business Continuity, Disaster Recovery, Continuity of Operations, Crisis Communications, Critical Infrastructure, Emergency Action, etc.
- D.** Implement an incident handling capability for security incidents that:
 - 1. Includes preparation, detection and analysis, containment, eradication, and recovery;
 - 2. Coordinates incident handling activities with contingency planning activities;
 - 3. Incorporates lessons learned from ongoing incident handling activities into incident response procedures, training, and testing/exercises, and implements the resulting changes accordingly; and
 - 4. Employs automated mechanisms to support the incident handling process.
- E.** Track and document information system security incidents.
- F.** Implement an incident reporting requirement of personnel that:
 - 1. Ensures incidents are reported to the Service Desk within 24 hours of occurrence;
 - 2. Ensures SITSD reports enterprise security incident information to Executive staff, the Information Technology Managers Council, Information Security Advisory Council, and the Legislative Audit Division on a monthly basis; and
 - 3. Employs automated mechanisms to assist in the reporting of security incidents.
- G.** Utilize the SITSD Service Desk, SITSD Information Systems Security Office, National Guard, MS-ISAC, Fusion Center and State Risk Management and Tort Claims Division as an incident response support resource that:

1. Provides support and assistance for handling incidents; and
 2. Ensures automated mechanisms are employed to increase the availability of incident response related information and support.
- H. Develop an ISIRT (Information Systems Incident Response Team) Manual that:
1. Provides a roadmap for implementing its incident response capability;
 2. Describes the structure and organization of the incident response capability;
 3. Provides a high-level approach for how the incident response capability fits into agency processes,
 4. Meets the requirements of mission, size, structure, and functions of the agency;
 5. Defines reportable incidents;
 6. Provides metrics for measuring the incident response capability for the agency;
 7. Defines the resources and management support needed to effectively maintain and mature an incident response capability;
 8. Establishes management review and approval of the ISIRT on a quarterly basis or to address system/organizational changes or problems encountered during implementation, execution, or testing ;
 9. Ensures distribution of updated versions is delivered to ISIRT members; and
 10. Protects the ISIRT from unauthorized disclosure and modification.

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](#)