

	Montana Operations Manual <i>POLICY TEMPLATE</i>	Category	Security
		Effective Date	
		Last Revised	
Issuing Authority	Department of Administration State Information Technology Services Division		
POL–Recover 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 (Recover Capabilities Policy) for defining actions to fulfill the responsibility. The POL- Recover Capabilities Policy serves to develop and implement the appropriate activities to maintain plans for resilience and to restore capabilities or services that were impaired due to 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 contingency plans and procedures for each information system that:
 1. Adhere to established contingency planning requirements through the [POL-State Government Continuity Program](#);
 2. Defines essential mission and business functions and associated contingency requirements;
 3. Addresses maintaining essential mission and business functions despite disruption, compromise, or failure;
 4. Addresses eventual, full information system restoration, without deterioration, of the security safeguards originally planned and implemented;
 5. Establishes recovery objectives, restoration priorities, and metrics;
 6. Addresses roles, responsibilities, and assigned individuals with contact information;
 7. Ensures distribution of copies of the contingency plan to key contingency personnel;
 8. Coordinates contingency planning activities with incident handling activities;
 9. Schedules a review of the contingency plan for the information systems annually;
 10. Requires revision of the contingency plan to address changes to State governance, information system, or environment of operation and problems encountered during implementation, execution, or testing;
 11. Ensures communication of contingency plan changes to key contingency personnel occurs;
 12. Requires review and approval by the appropriate agency authorizing official; and
 13. Protects the contingency plan from unauthorized disclosure and modification.
- B.** Conduct appropriate training through the state continuity program and other training opportunities.
- C.** Conduct appropriate contingency plan testing through the state continuity program, agency continuity program, SITSD, and/or other testing programs.
- D.** Maintain an offsite storage site to be in place and used for essential business functions.
- E.** Ensure an alternative processing site is in place and can be used for essential business functions.

- F. Ensure alternate telecommunication services are available for essential mission and business functions at primary and alternate processing storage sites.
- G. Conduct backups of user-level and system-level information contained in the information system as defined by the data owner.
- H. Provide for the recovery and reconstitution of systems, including transaction recovery, to a known state after disruption, compromise, or failure.

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](#)