

	Montana Operations Manual <i>POLICY TEMPLATE</i>	Category	Security
		Effective Date	
		Last Revised	
Issuing Authority	Department of Administration State Information Technology Services Division		
POL–Identify 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-Identify Capabilities Policy serves to develop the institutional understanding to manage cybersecurity risk to enterprise systems, assets, data, and capabilities.

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.** Maintain an inventory of information system components. Inventory of systems is conducted annually and reviewed for any unauthorized components. Unauthorized components are removed.
- B.** Map organizational communication and data flows by:
 - 1. Approving flow of information between information systems;
 - 2. Requiring an Interconnection Security Agreement for all information systems directly connected to external systems;
 - 3. Outlining connections with other information systems within the system security plan;
 - 4. Employing a permit-by documented request (exception) policy for allowing agency and other information systems to connect to external information system; and
 - 5. Ensuring that all internal connections for an information system are documented within the system security plan.
- C.** Maintain agreements with external entities when using external information systems to use, process, store, or transmit state data that includes the following:
 - 1. Ensuring compliance with access requirements;
 - 2. Requiring that providers of external information system services comply with organizational information security requirements and employ appropriate security in accordance with applicable state laws, Executive Orders, policies, standards, and guidance;
 - 3. Defining and documenting State of Montana oversight and user roles and responsibilities with regard to external information systems;
 - 4. Monitoring security control compliance by external service providers; and
 - 5. Requiring providers of information system services to identify the functions, ports, protocols, and other services required for the use of such services.
- D.** Establish cybersecurity roles and responsibilities for the entire workforce and third-party stakeholders (e.g., suppliers, customers, partners).
- E.** Establish dependencies, critical functions, and requirements, for delivery of critical services.
- F.** Establish and maintain information security policies that provide the following:

1. Coordination and alignment of information security roles and responsibilities with internal roles and external partners;
2. Ensure that legal and regulatory requirements regarding information security, including privacy and civil liberties obligations, are understood and managed; and
3. Ensure governance and risk management processes address information security risks.

G. Identify and document asset vulnerabilities by:

1. Obtaining, protecting as required, and making available to authorized personnel, administrator documentation for the information system that describes:
 - Secure configuration, installation, and operation of the information system;
 - Effective use and maintenance of security features/functions; and
 - Known vulnerabilities regarding configuration and use of administrative (i.e., privileged) functions.
2. Obtaining, protecting as required, and making available to authorized personnel, user documentation for the information system that describes:
 - User-accessible security features/functions and how to effectively use those security features/functions;
 - Methods for user interaction with the information system, which enables individuals to use the system a more secure manner; and
 - User responsibilities in maintaining the security of the information and information system.
3. Documenting attempts to obtain information system documentation when such documentation is either unavailable or nonexistent;
4. Protecting documentation as required in accordance with the risk management strategy;
5. Scanning for vulnerabilities in information systems and hosted applications annually and when new vulnerabilities potentially affect the system/applications are identified and reported;
6. Employing vulnerability scanning tools and techniques that promote interoperability among tools and automating parts of the vulnerability management process by using standards for:
 - Enumerating platforms, software flaws, and improper configurations;
 - Formatting and making transparent, checklists and test procedures; and;

- Measuring vulnerability impact;
- 7. Analyzing vulnerability scan reports and results from security control assessments;
- 8. Remediating critical vulnerabilities within thirty (30) business days in accordance with an organizational assessment of risk;
- 9. Sharing information obtained from the vulnerability scanning process and security control assessments with designated personnel to help eliminate similar vulnerabilities in other information systems;
- 10. Employing a vulnerability scanning tool that automates vulnerability list updates at least weekly, prior to a new scan, and when new vulnerabilities are identified and reported;
- 11. Authorizing privileged access for vulnerability scanning activities;
- 12. Requiring that information system developers/integrators:
 - Create and implement a security test and evaluation plan;
 - Implement a verifiable flaw remediation process to correct weaknesses and deficiencies identified during the security testing and evaluation process;
 - Document the results of the security testing/evaluation and flaw remediation processes.

H. Receive security alerts, advisories, and directives that:

1. Originate from designated trusted external organizations;
2. Are communicated on an ongoing basis;
3. Generate internal security alerts, advisories, and directives as deemed necessary;
4. Are disseminated to appropriate entity/agency security contracts for their use and distribution;
5. Are used to implement security directives in accordance with established time frames, or notifies the issuing organization of the degree of noncompliance;
6. Are used to facilitate ongoing security education and training for organizational personnel;
7. Assist with maintaining currency with recommended security practices, techniques, and technologies;
8. Include current threats, vulnerabilities, and incidents; and
9. Are used to implement a threat awareness program that includes a cross-organization information-sharing capability.

I. Conduct risk assessments that include the following:

1. The likelihood and magnitude of harm, from unauthorized access, use, disclosure, disruption, modification, or destruction of information systems and the information it processes, stores, or transmits;
 2. Documentation of the risk assessment results in a risk assessment report;
 3. Annual review of the risk assessment results; and
 4. Annual updates or whenever there are significant changes to information systems or environment of operation (including the identification of new threats and vulnerabilities), or other conditions that may affect the security state of the system.
- J.** Establishes security categorizations that:
1. Are in accordance with applicable state laws, Executive Orders, directives, policies, standards, and guidance;
 2. Are documented within the security plan for each information system; and
 3. Ensures the authorizing official or designated representative reviews and approves of the security categorization decision.
- K.** Implement a process for ensuring that plans of action and milestones for the security program and the associated organizational information systems are:
1. Developed and maintained;
 2. Contain documentation of the remedial information actions to mitigate risk to organizational operations and assets, individuals, other organizations, and the State; and
 3. Reported in manner consistent with State of Montana (OMB FISMA) requirements.
- L.** Develop and implement a comprehensive and consistent strategy to manage risk to organizational operations and assets, individuals, other organizations, and the State associated with the operation and use of information systems that includes the following:
1. Establishing and communicating priorities for organizational mission, objectives and activities;
 2. A determination of organizational risk tolerance that is clearly expressed and communicated;
 3. A definition of mission/business processes with consideration for information security and the resulting risk to organizational operations, organizational assets, individuals, other organizations, and the State;
 4. A determination of information protection needs arising from the defined mission/business processes and revision to the processes as necessary, until an achievable set of protection needs is obtained; and
 5. Development, documentation, and updating of critical infrastructure and key resources protection plan.

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](#)