

	Montana Operations Manual <i>POLICY TEMPLATE</i>	Category	Security
		Effective Date	
		Last Revised	
Issuing Authority	Department of Administration State Information Technology Services Division		
POL–Protect 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 safeguards, prioritized through the organization’s risk management process, to ensure delivery of critical infrastructure services.

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. Manage identities and credentials for authorized devices and users that:

1. Provides unique identification and authentication to information systems;
2. Employs the use of multifactor authentication for access to privileged accounts;
3. Provides unique identification and authentication to all network attached devices compatible with the 802.1X protocol prior to establishing a network connection;
4. Provides unique information system identifiers (UserID)s by:
 - Requesting the identifier from SITSD;
 - Receiving authorization from an authorizing manager;
 - Selecting an identifier that identifies an individual, group role, or device;
 - Assigning the identifier to the intended individual group, role, or device; and
 - Prohibiting the reuse of identifiers.
5. Requires the following of identifiers:
 - Password have a minimum of eight (8) characters that contain lower case and upper case letters and numbers;
 - Password must be changed upon first login;
 - Password changes are required every sixty (sixty) days;
 - Password encryption during both storage and transmission;
 - Password reuse is prohibited for six (6) generations; and
 - Follows developed agency documented provisioning and de-provisioning processes.
6. Requires that certificates are validated and map the identity to the user account;
7. Requires that hardware token-based authentication employs mechanisms that satisfy Public Key Infrastructure (PKI) requirements;
8. Obscures feedback of authentication information during the authentication process to protect the information from possible exploitation/use by unauthorized individuals;
9. Employs cryptographic authentication, on systems with sensitive information, that complies with requirements set forth by applicable policies, standards, and guidance;

10. Identifies and authenticates non-organizational users using federated identify mechanisms (ePass) that allows authentication to some external platforms and services;
11. Identifies information system accounts by type e.g., individual, shared, group, system, guest/anonymous, emergency, developer, manufacturer, vendor, temporary, and service;
12. Assigns account managers for information system accounts;
13. Establishes conditions for group and role membership;
14. Specifies authorized users of the information system, group and role memberships, and access authorizations (i.e., privileges) and other attributes (as required) for each account;
15. Requires approvals by system owners, a contract manager, or business manager for requests to create information system accounts;
16. Creates, enables, modifies, disables, and removes information system accounts in accordance with account managers;
17. Monitors the use of, information system accounts;
18. Employs automated mechanisms to support the management of information system accounts;
19. Automates the disabling of temporary and emergency accounts after sixty (60) days;
20. Automates the disabling of inactive accounts and identifiers after ninety (90) days; and
21. Automates the auditing and provides notification to account managers the following account actions:
 - Creation
 - Modification
 - Enabling
 - Disabling
 - Removal

B. Notify account managers through the information system owner when:

1. Accounts are no longer required;
2. Users are terminated or transferred; and
3. Individual information system usage or need-to-know changes.

C. Authorize access to information systems based on:

1. Valid access authorization;
2. Intended system usage; and

3. Other attributes as required by the mission\business function.

D. Manage and protect physical access to assets that:

1. Require a current list of personnel with authorized access to the facilities where information systems reside;
2. Require the issuance of authorization credentials;
3. Require the review and approval of the access list and authorization credential on a monthly basis;
4. Remove personnel from the access list that no longer require access;
5. Enforce physical access authorizations for all physical access points where the information system resides;
6. Verify individual access authorizations before granting access to facilities;
7. Control entry to facilities containing the information systems using physical access controls;
8. Control access to areas officially designated as publicly accessible in accordance with the organization's assessment of risk;
9. Secure keys, combinations, and other physical access devices;
10. Inventory physical access devices annually;
11. Change combinations and keys when keys are lost, combinations are compromised, or individuals are transferred or terminated.
12. Control physical access to information system distribution and transmission within state facilities;
13. Control physical access to sensitive information system output devices to prevent unauthorized individuals from obtaining the output;
14. Monitor physical access by:
 - Detecting and responding, in real time, to physical security incidents;
 - Reviewing physical access logs monthly; and
 - Coordinating results of reviews and investigations with the state's incident response capability.
15. Maintain visitor access records to facilities that house sensitive information systems and reviews visitor access records monthly; and
16. Protect power equipment and power cabling for sensitive information from damage and destruction.

E. Manage Remote Access that:

1. Maintains usage restriction, configuration requirements, and implementation guidance;

2. Requires multifactor authentication;
3. Requires authorization from the information system owner;
4. Monitors all access sessions;
5. Utilizes encryption;
6. Routes traffic through SITSD enterprise designated control points;
7. Restricts the use of privileged commands to system administrators;
8. Maintains terms and conditions for the use of mobile device to access state information systems; and
9. Requires that agreements are established with external entities when utilizing external information systems to use, process, store or transmit state data.

F. Manage access permissions that:

1. Incorporates the principle of least privilege according to mission and business function;
2. Incorporates and documents the principle of separation of duties; and
3. Approves access to State systems.

G. Protect network integrity by:

1. Approving flow of information between information systems;
2. Monitoring and controlling communications at the external boundary of the system and at key internal boundaries within the system;
3. Connecting to external networks or information systems only through managed interfaces consisting of boundary protection devices arranged in accordance with security architecture;
4. Allocating publicly accessible State of Montana network components to separate sub-network with separate physical network interfaces;
5. Preventing public access into the State of Montana's internal networks except as appropriately mediated by managed interfaces employing boundary protection devices;
6. Limiting the number of access points to the State of Montana network to allow for more comprehensive monitoring of inbound and outbound communications and network traffic;
7. Implementing a managed interface for each external telecommunication service;
8. Establishing a traffic flow ruleset for each managed interface that denies network traffic by default and allows network traffic by exception (i.e., deny all, permit by exception);

9. Employing security controls as needed to protect the confidentiality and integrity of the information being transmitted;
 10. Documenting each exception to the traffic flow policy with supporting mission/business need and duration of that need;
 11. Reviewing exceptions to the traffic flow ruleset annually or upon request;
 12. Removing traffic flow policy exceptions that are no longer supported by an explicit mission/business need; and
 13. Preventing remote devices that have established a non-remote connection with the system from communicating outside of that communications path with resources in external networks.
- H.** Provide State of Montana personnel and partners cybersecurity awareness education that:
1. Includes basic security awareness training to new employees prior to provisioning access to systems or performance of duties;
 2. Requires annual security awareness training to all other staff members including managers, senior executives, and contractors; and
 3. Requires that privileged users understand and acknowledge their roles and responsibilities
- I.** Manage information and records consistent with the organization's risk strategy to protect confidentiality, integrity, and availability that:
1. Employs appropriate security technologies for data-at-rest;
 2. Employs cryptographic mechanisms to recognize changes to information during transmission unless otherwise protected by alternative physical measures;
 3. Requires assets are formally managed by:
 - Maintaining an inventory of information system components;
 - Conducting annual reviews of information system inventory;
 - Removing unauthorized components;
 - Sanitizing sensitive information system media (both digital and non-digital), with sanitization mechanisms that are commensurate with the classification or sensitivity of the information, prior to disposal, release of organizational control, or reuse; and
 - Authorizing, monitoring, and controlling servers, server racks, hard drives, workstations, network arrays, network equipment, and any other pertinent equipment entering and exiting secured data center facilities and maintaining records of those items.
 4. Maintains adequate capability and capacity to ensure availability by:
 - Allowing flexibility in audit storage capacity; and

- Protecting against or limiting the effects of denial of service attacks.
5. Protects against data leaks by:
 - Approving flow of information between information systems;
 - Documenting separation of duties;
 - Employing the principle of least privilege according to mission/business functions;
 - Screening individuals prior to authorizing access to information systems and rescreening individuals according to the following conditions:
 - Job Transfer/Hire into a position that require additional security/privileged access; and
 - Every three (3) years.
 - Ensuring that individuals who have access to organizational sensitive information, sign appropriate access agreements prior to being granted access;
 - Reviewing and updating access agreements every two (2) years;
 - Employing boundary protection mechanisms;
 - Employing cryptographic mechanisms, protections, and modules that comply with applicable state laws, Executive Orders, policies, standards and guidance;
 - Monitoring events by:
 - Utilizing security incident and event monitoring objectives to detect information system attacks; and
 - Identifying unauthorized use of information systems;
 6. Detects unauthorized changes to software and information, and reassesses the integrity of software and information by performing integrity scans of the information system on an annual basis; and
 7. Maintains separate development and testing environments along with baseline configuration for rollback support.
- J.** Create and maintain a baseline configuration of information technology systems that:
1. Requires a review bi-annually or as needed;
 2. Retains older versions of baseline configurations for rollback support;
 3. Employs a formal change management system that includes the following:
 - Types of changes that need to be documented in the tool;
 - Approval process that includes security review;

- Documentation of approved changes;
- Retention records of changes and review processes;
- Auditing of change activities;
- Coordination and oversight capabilities for configuration change control activities;
- Capability to approve, hold until approved, and document the completion of requested changes; and
- Processes to test, validate, and document changes prior to implementation.

4. Requires testing, validation, and documentation prior to implementation of changes in order to determine potential security impacts;
5. Requires review by appropriate security staff prior to change implementation;
6. Restricts physical and logical access for changes to appropriate staff;
7. Maintains mandatory configuration settings for each information system;
8. Requires approval and documentation of exceptions to mandatory settings;
9. Maintains the principle of least functionality. That is, information system functions, ports, protocols, and/or services are limited where applicable; and
10. Employs a configuration management plan.

K. Manage information systems using a system development lifecycle methodology that:

1. Includes information security considerations;
2. Defines and documents information system security roles and responsibilities throughout the system development lifecycle; and
3. Identifies individuals having information system security roles and responsibilities.
4. Requires information system acquisition contracts include the following:
 - Security functional requirements/specifications;
 - Security-related documentation requirements;
 - Developmental and evaluation-related assurance requirements;
 - Functional properties of the security controls to be employed within information systems, information system components, or information system services in sufficient detail to permit analysis and testing of the controls;

- Security-relevant external system interfaces and high-level design;
 - Identification of the functions, ports, protocols, services intended for organization use.
 - Information technology products are on the FIPS 201-approved product list for Personal Identify Verification (PIV).
5. Includes system security engineering principles in the specification, design, development, implementation, and modification of the information system;
 6. Requires information system developers/integrators perform the following:
 - Configuration management during information system design, development, implementation, and operation;
 - Management and control changes to the information system;
 - Implementation of only organization-approved changes;
 - Documentation of approved changes to the information system;
 - Tracking of security flaws and flaw resolution;
 - Creation of a security test and evaluation plan;
 - Implementation of a verifiable flaw remediation process to correct weaknesses and deficiencies identified during the security testing and evaluation process; and
 - Documentation of the security testing/evaluation and flaw remediation processes.
 7. Requires development of an information security architecture for the information system that:
 - Describes the overall philosophy, requirements, and approach to be taken with regard to protecting the confidentiality, integrity, and availability of organizational information;
 - Describes how the information security architecture is integrated into and supports the enterprise architecture;
 - Describes any information security assumptions about, and dependencies on, external services;
 - Reviews and updates the information security architecture every two years to reflect updates in the enterprise architecture; and
 - Ensures that planned information security architecture changes are reflected in the operational security plan and organizational procurements/acquisitions.
- L.** Maintain a physical operating environment for state assets that:
1. Provides for the following emergency shutoff capabilities:

- Shutting off power to sensitive information systems or individual system components in emergency situations;
 - Placement of emergency shutoff switches or devices in appropriate locations within secured facilities to facilitate safe and easy access for personnel;
 - Protection of emergency power shutoff capability from unauthorized activation;
2. Provides a short-term uninterruptible power supply to facilitate an orderly shutdown of information systems in the event of a primary power source loss; and
 3. Employs automatic emergency lighting for information systems that activates in the event of a power outage or disruption and that covers emergency exits and evacuation routes within facilities;
 4. Provides for the following fire protection capabilities:
 - Fire suppression and detection systems for sensitive information systems that are supported by an independent energy source;
 - Fire detection systems for sensitive information systems that activates automatically and notifies authorized personnel and emergency responders in the event of a fire;
 - Fire suppression systems for sensitive information systems that provides automatic notification for any activation State emergency responders; and
 - Fire suppression system for sensitive information systems in unstaffed facilities.
 5. Maintains temperature and humidity levels within the facilities where sensitive information resides between 68-71 degrees Fahrenheit and humidity can be anywhere from 28% to 54%; temperature and humidity levels are monitored 24/7;
 6. Protects sensitive information systems from damage resulting from water leakage by ensuring a master shutoff valve is accessible, working properly, and known to key personnel; and
 7. Authorizes, monitors, and controls servers, server racks, hard drives, workstations, network arrays, network equipment, and any other pertinent equipment entering and exiting secured data center facilities and maintains records of those items.
- M.** Sanitize sensitive information system media (both digital and non-digital) prior to disposal, release of organizational control, or reuse. NOTE: Employed sanitization mechanisms (strength and integrity) must be commensurate with the classification and sensitivity of the information.
- N.** Continuously improve protection processes by:

1. Creating a formal System Security Plan that:
 - Is consistent with the organization's enterprise architecture;
 - Explicitly defines the authorization boundary for the system;
 - Describes the operational context of the information system in terms of mission and business processes;
 - Provides the security categorization of the information system including supporting rationale;
 - Describes the operational environment for the information system and relationships with or connections to other information systems;
 - Provides an overview of the security requirements for the system;
 - Identifies any specific statutory and/or regulatory requirements (above and beyond Moderate Baseline Controls), if applicable;
 - Describes the security controls in place or planned for meeting those requirements including a rationale for the tailoring and supplementation decisions; and
 - Is reviewed and approved by the authorizing official or designated representative prior to plan implementation.
2. Distributing copies of the System Security Plan and communicating changes to the plan to appropriate personnel;
3. Reviewing the System Security Plan for the information system at least once every year;
4. Updating the System Security Plan to address changes to the information system/environment of operation or problems identified during plan implementation or security control assessments;
5. Protecting the System Security Plan from unauthorized disclosure and modification;
6. Planning and coordinating security-related activities with other organizational entities before conducting such activities in order to reduce the impact on enterprise operations, for example, security assessments, audits, hardware and software maintenance, patch management, and contingency plan testing.
7. Developing, monitoring, and reporting on the results of information security measures of performance.
8. Developing a continuous monitoring strategy and implementing a continuous monitoring program that:
 - Establishes metrics to be monitored;
 - Establishes frequencies for monitoring and frequencies for assessments supporting such monitoring;

- Develops ongoing security control assessments in accordance with the agency continuous monitoring strategy;
 - Develops ongoing security status monitoring of agency-defined metrics;
 - Correlates and analyzes security-related information generated by assessments and monitoring;
 - Develops response actions to address results of the analysis of security related information;
 - Reports the security status of the agency and information systems to agency-defined personnel within agency-defined frequency; and
 - Employs assessors or assessment teams with an agency-defined level of independence to monitor the security controls in the information system on an ongoing basis.
9. Sharing the effectiveness of protection technologies with appropriate parties.
10. Ensuring that response plans (Incident Response and Business Continuity) and recovery plans (Incident Recovery and Disaster Recovery) are in place and managed.
11. Ensuring that response and recovery plans are tested.
12. Ensuring that cybersecurity is included in human resources practices that:
- Assigns a risk designation to all positions and establishes screening criteria for individuals filling those positions;
 - Reviews and revises position risk designations every two years;
 - Upon termination of individual employment the agency shall:
 - Terminate all information system access;
 - Conduct exit interviews;
 - Retrieve all security-related organizational information system-related property; and
 - Retain access to organizational information and information systems formerly controlled by terminated individual.
 - Upon reassigning or transferring agency personnel to other positions within the State, agencies shall conduct a review of logical and physical access authorizations to information systems/facilities within three business days of beginning the new position to ensure access is limited to authorized and required systems/facilities.
 - Establishes third-party personnel security requirements that:
 - Includes security roles and responsibilities for the providers;

- Documents personnel security requirements; and
- Monitors provider compliance.
- Employs a formal sanctions process for personnel failing to comply with established information security policies and procedures.

13. Developing and implementing a vulnerability management plan.

O. Maintain and repair organization assets by:

1. Utilizing a formalized change management process;
2. Performing maintenance on major equipment that contains sensitive information on-site;
3. Performing security checks that are performed after maintenance is completed;
4. Approving, controlling, monitoring the use of, and maintaining on an ongoing basis, information system maintenance tools;
5. Checking information system maintenance tools prior to admittance into a secured data center facility;
6. Checking all media for virus or malicious code before it is used on an information system;
7. Establishing a process for maintenance personnel authorization by maintaining a current list of authorized maintenance organizations or personnel; and
8. Ensuring that personnel performing maintenance on an information system that contains sensitive information have had a background check.

P. Perform remote maintenance of organizational assets in a secure manner by:

1. Authorizing, monitoring, and controlling all non-local maintenance and diagnostic activities;
2. Allowing the use of non-local maintenance and diagnostic tools only as consistent with organizational policy and documented in the system security plan for the information system;
3. Employing strong identification and authentication techniques in the establishment of non-local maintenance and diagnostic sessions;
4. Maintaining records for non-local maintenance and diagnostic activities; and
5. Terminating all session and network connection when non-local maintenance is completed.

Q. Manage information system audit/log records by:

1. Ensuring audit logs contain the following events:
 - System Access;

- Alterations to user account rights and permissions;
 - System security logs;
 - Privileged functions; and
 - Other system owner identified events.
2. Reviewing and updating the list of auditable events on an annual basis;
 3. Ensuring audit records that are able to identify the following:
 - Type of event;
 - Date and time of event;
 - Location of event;
 - Source of event;
 - Success or failure of event (if applicable); and
 - User or subject associated with the event.
 4. Maintaining a storage area for audit records that allows flexibility in the size of information collected;
 5. Providing automatic alerting to system owners for audit processing failures;
 6. Requiring administrators to stop audit record generation if a failure in audit processing occurs;
 7. Reviewing audit records on a monthly basis unless otherwise specified in the audit procedures. Reviews are adjusted as needed depending upon the identification of possible attacks or pain points within information systems. Reports are generated to identify suspicious activity. Data is correlated across different repositories to gain organization-wide situational awareness;
 8. Providing for an audit reduction and report generation capability based on selected event criteria;
 9. Generating time stamps for audit records using the external naval clock time process;
 10. Accessing audit information and tools is limited to those whose job duties require access or the staff members who are performing the audit function;
 11. Maintaining audit records for minimum of six (6) years to meet regulatory requirements; and
 12. Ensuring that information systems can provide audit record generation capability for the auditable events defined in this section.

R. Protect removable media by:

1. Restricting access to raised-floor areas that contain critical network, data backup, and server functions to authorized users, vendors, and customers using automated physical security restrictions and biometrics (where deployed);
 2. Controlling and storing failed or retired hard drives and tape media that contains sensitive information within designated secure areas within facilities using physical control restrictions;
 3. Protecting sensitive information system media until the media is destroyed or sanitized using approved equipment, techniques, and procedures;
 4. Protecting and controlling sensitive information media during transport outside of controlled areas using authorized personnel and secured transport;
 5. Maintaining accountability for sensitive information system media during transport outside of controlled areas;
 6. Restricting the activities associated with transport of such media to authorized personnel;
 7. Documenting activities associated with the transport of sensitive information system media;
 8. Employing cryptographic mechanisms to protect the confidentiality and integrity of sensitive information stored on digital media during transport outside of controlled areas; and
 9. Prohibiting the use of portable storage devices in organizational information systems when such devices have no identifiable owner.
- S.** Control access to systems and assets, incorporating the principle of least functionality by:
1. Ensuring that the respective State system owner approves access to State systems;
 2. Reviewing information system functions, ports, protocols, and/or services are limited where applicable;
 3. Maintaining an enterprise list of software (exceptions, white and black list);
 4. Conducting an annual inventory of systems for any unauthorized software use; and
 5. Removing unauthorized software.
- T.** Protect communication and control networks by:
1. Approving the flow of information between information systems;
 2. Maintaining usage restrictions, configuration requirements, and implementation guidance for wireless access that;
 - Authorizes wireless access connections by the information system owner;

- Authenticates wireless access users and devices; and
 - Encrypts wireless access.
3. Maintaining alternate telecommunication services for essential mission and business functions at primary and alternate processing and storage sites.

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](#)