POL-Information Security Policy
APPENDIX A
STATE OF MONTANA
BASELINE SECURITY CONTROLS

Common Security Controls Baseline = MODERATE

NIST 800-53 defines Common Controls as, "security controls that are inheritable by one or more organizational information system". This document provides a list of security controls at the Moderate level as presented in NIST SP 800 53, Rev 4. The State Information Technology Services Division of Montana has structured security controls for all systems managed by SITSD for state-wide application and use to this Moderate level as the baseline or standard practice for SITSD managed state IT asset security architecture. This document will be used in collaboration with state agencies in identifying a common approach to implementation of baseline security controls for all state agencies.

The following is a table of the various security control categories established by NIST 800-53. The State of Montana implements security controls for all information systems based on appropriate risk-based analysis in accordance with NIST guidelines.

Identifier	Family	Core Function
AC	Access Control	Identify, Protect, Detect
AT	Awareness and Training	Protect
AU	Audit and Accountability	Protect, Detect, Respond
CA	Security Assessment and Authorization	Identify, Protect, Detect, Respond
CM	Configuration Management	Identify, Protect, Detect
CP	Contingency Planning	Identify, Protect, Detect, Respond, Recover
IA	Identification and Authentication	Protect
IR	Incident Response	Protect, Detect, Respond, Recover
MA	Maintenance	Protect
MP	Media Protection	Protect
PE	Physical and Environmental Protection	Identify, Protect, Detect Respond
PL	Planning	Identify, Protect, Detect
PS	Personnel Security	Identify, Protect, Detect
RA	Risk Assessment	Identify, Protect, Detect, Respond
SA	System and Services Acquisition	Identify, Protect, Detect
SC	System and Communications Protection	Protect, Detect
SI	System and Information Integrity	Identify, Protect, Detect, Respond
PM	Program Management	Identify, Protect, Detect, Respond

State Enterprise policies may be referenced for use by state directorates/agencies. State agencies may also adopt the use of other agency policies where direct application may support similar agency requirements.

FAMILY/Category: Access Control (AC)

Control Number	Control Name	Priority	Initial Control Baseline
AC-1	Access Control Policy and Procedures	P1	AC-1

The State of Montana reviews and updates Access Control policies and procedures within two years of last review.

Each Agency shall ensure that an organization structure is in place to:

1. assign information security responsibilities;
2. perform Access Control for Information Systems;
3. allocate adequate resources to implement Access Controls;
4. develop processes and procedures to measure compliance

Control Number	Control Name	Priority	Control Baseline
AC-2	Account Management	P1	AC-2 (1) (2) (3) (4)

Information system accounts for the State of Montana have the following management requirements:

a. identified by type
b. assigned account managers
c. have established conditions for group and role membership
d. Specifies access privileges and other attributes
e. Requires approval by system owner, a contract manager, or business manager to create
f. are created, modified, disabled, or removed by account managers
g. monitored if they are temporary or guest accounts
h. are reviewed on an annual basis for compliance with requirements
i. disabled when no longer needed or if not used for 90 days

The Information system owner notifies account managers:

a. When accounts are no longer required
b. When users are terminated or transferred; and
c. When individual information system usage or need-to-know changes.

These notifications must be documented.
The information system owner authorizes access to the information system based on:

a. A valid access authorization
b. Intended system usage; and
c. Other attributes as required by the mission\business function

Auditing occurs for account creation, modification, enabling, disabling and removal actions (e.g., Change Auditor).

Control Number	Control Name	Priority	Control Baseline
AC-3	Access Enforcement	P1	AC-3

The respective State system owner approves access to State systems.

Control Number	Control Name	Priority	Control Baseline
AC-4	Information Flow Enforcement	P1	AC-4

The respective State system approves flow of information between information systems.

Control Number	Control Name	Priority	Control Baseline
AC-5	Separation of Duties	P1	AC-5

The State of Montana employs documented separation of duties for information systems.

Control Number	Control Name	Priority	Control Baseline
AC-6	Least Privilege	P1	AC-6 (1)(2) (5)(9)(10)

The State of Montana employs the use of least privilege according to organizational mission and business function.

Users will be assigned to the most restrictive type of account that only allows them to perform their primary job functions.

Control Number	Control Name	Priority	Control Baseline
AC-7	Unsuccessful Logon Attempts	P2	AC-7

The State of Montana enforces a limit of 6 consecutive invalid login attempts by a user during a 30-minute period. When the 6 attempts are exceeded, accounts are automatically locked out for a period of 8 hours or until an administrator releases the account.

Control Number	Control Name	Priority	Control Baseline
AC-8	System Use Notification	P1	AC-8

All state computers used by a state employee or state contractor must have a warning banner displayed at all access points. This banner must warn authorized and unauthorized users of the following:

1. what is considered the proper use of the system,
2. that the system is being monitored to detect improper use and other illicit activity, and
3. that there is no expectation of privacy while using the system.

At a minimum, all internal State Information Systems, including portal access systems, will display one of the following notification banners before granting access to the system:

Mainframe:

This computer system is the property of the State of Montana and is subject to the use policies located at:

http://mom.mt.gov

This computer system contains sensitive U.S. and State government information and is limited to authorized personnel only. Authorized personnel may inspect any uses of this system. By using this system, the user consents to such inspection at the discretion of authorized personnel.

Unauthorized access is a violation of state law 45-6-311, MCA, and prohibited by Public Law 99-474, Title 18, United States Code, Public Law 99-474 and Chapter XXI, Section 1030. Unauthorized use of this system may result in disciplinary action, civil and criminal penalties. Federal punishment may include fines and imprisonment for not more than 10 years, or both. By using this system you indicate your consent to these terms and conditions of use. Log off immediately if you do not agree to these conditions.

Network Devices:

This computer, provided only for authorized State government use, is the property of the State of Montana. Any use of this system and all files on this system may be intercepted, monitored, recorded, copied, audited, inspected, and disclosed to authorized personnel. Unauthorized or improper use of this system may result in administrative disciplinary action and civil and criminal penalties. Log off immediately if you do not agree to the conditions stated in this warning.

Network Login including remote access:

This computer is the property of the State of Montana and subject to the appropriate use policies located at mom.mt.gov. Unauthorized use is a violation of 45-6-311, MCA. This computer system, including all related equipment, networks, and network devices, is provided only for authorized State government use. Any or all uses of this system and all files on this system may be intercepted, monitored, recorded, copied, audited, inspected and disclosed to authorized personnel. By using this system, the user consents to such interception, monitoring, recording, copying, auditing, inspection, and disclosure at the discretion of authorized personnel. Unauthorized or improper use of this system may result in administrative disciplinary action and civil and criminal penalties. By continuing to use this system, you indicate your awareness of and consent to these terms and conditions of use. **Log off immediately** if you do not agree with the conditions stated in this warning.

Agency specific messages may be incorporated into these logon notifications to reflect their specific requirements.

Control Number	Control Name	Priority	Control Baseline
AC-11	Session Lock	P3	AC-11 (1)

All State information systems:

a. Prevent further access to the system by initiating a session lock after a maximum of twenty (15) minutes of inactivity or upon receiving a request from a user; and
b. Retain the session lock until the user reestablishes access using established identification and authentication procedures.

The information system conceals information previously visible on the display with a publicly viewable image.

Control Number	Control Name	Priority	Control Baseline
AC-12	Session Termination	P2	AC-12

All State information systems automatically terminate a user [logical] session after 20 minutes of inactivity unless mitigated by alternative controls, e.g., desktop lockout. *(related control is SC-10/Network and SC-23/Session Authenticity).*

Control Number	Control Name	Priority	Control Baseline
AC-14	Permitted Actions without Identification or Authentication	P1	AC-14 (1)

The system owner identifies and documents specific user actions not requiring identification or authentication.

Control Number	Control Name	Priority	Control Baseline
AC-17	Remote Access	P1	AC-17 (1) (2) (3) (4)

The State of Montana maintains usage restrictions, configuration requirements, and implementation guidance for remote access. Remote access is authorized by the information system owner.

Remote access is monitored and uses encryption for all access sessions. All remote access is routed through state designated control points (e.g., Helena & Billings). Privileged commands are authorized only for system administrators.

SITSD will provide a secured connection via dedicated Internet connection to access all state information technology resources. Agencies are to use only this connection for remote access into the state's information technology resources. The appropriate agency administrator must provide requests for remote access for each employee or contractor in writing to SITSD. SITSD will provide the agency with the procedures to be used so that their employee or contractor can connect to the state network. Remote access users are obligated to abide by all computing policies of the state and the agency. Access will be granted for legitimate business uses of the State of Montana and not for personal use. Access to the state's information technology resources by unauthorized remote users will be considered a violation of state policy. SITSD may grant exceptions to this policy to an agency if the secured remote service provided does not meet Federal or some other contract requirements. A full security review of the agency's proposed exception will be conducted by SITSD to ensure that the request and proposed solution meet enterprise security requirements.

Control Number	Control Name	Priority	Control Baseline
AC-18	Wireless Access	P1	AC-18 (1)

The state of Montana maintains usage restrictions, configuration requirements, and implementation guidance for wireless access. Wireless access is authorized by the information system owner.

Wireless access is protected by authentication of users and devices and uses NIST standard encryption for authentication and communication.

Control Number	Control Name	Priority	Control Baseline
AC-19	Access Control for Mobile Devices	P1	AC-19 (5)

The State of Montana has terms and conditions for the use of mobile devices to access state information systems.

All devices used to connect directly to state computers must be state owned.

Control Number	Control Name	Priority	Control Baseline
AC-20	Use of External Information Systems	P1	AC-20 (1) (2)

State Agencies have agreements with external entities when using external information systems to use, process, store, or transmit state data. State agencies are responsible for compliance with access requirements to these systems.

Control Number	Control Name	Priority	Control Baseline
AC-21	Information Sharing	P1	AC-21

The system owner facilitates information sharing by determining whether access authorization matches access restrictions. Any information sharing is reviewed before being released to sharing partners to ensure appropriate content is being provided.

Control Number	Control Name	Priority	Control Baseline
AC-22	Publicly Accessible Content	P2	AC-22

The system owner manages publicly accessible state generated content by reviewing it before it is posted for public access.

FAMILY/Category: Awareness and Training (AT)

Control Number	Control Name	Priority	Control Baseline
AT-1	Security Awareness and Training Policy & Procedures	P1	AT-1

The State of Montana reviews and updates Security Awareness and Training policies and procedures within two years of last review.

Control Number	Control Name	Priority	Control Baseline
AT-2	Security Awareness Training	P1	AT-2

The State of Montana provides basic security awareness training to new employees, as well as annual security training to all other staff members including managers, senior executives, and contractors.

Control Number	Control Name	Priority	Control Baseline
AT-3	Role-Based Security Training	P1	AT-3

The State of Montana provides security training to staff before providing access to systems or performing assigned duties.

Control Number	Control Name	Priority	Control Baseline
AT-4	Security Training Records	P3	AT-4

The State of Montana maintains security training records for minimum of 10 years after the employee is terminated or leaves state employment (RE: SoS GS-5, 26 & 29).

FAMILY/Category: Audit and Accountability (AU)

Control Number	Control Name	Priority	Control Baseline
AU-1	Audit and Accountability Policy & Procedures	P1	AU-1

The State of Montana reviews and updates Audit and Accountability policies and procedures within two years of last review.

Control Number	Control Name	Priority	Control Baseline
AU-2	Auditable Events	P1	AU-2 (3)

The State of Montana maintains audit logs that contain the following events:

- System Access
- Alterations to user account rights and permissions
- System security logs
- Privileged functions (e.g., Network Admin)
- Other system owner identified events
- Modifications to production application/system software
- Modifications to hardware

The State of Montana reviews and updates the list of auditable events on an annual basis.

Control Number	Control Name	Priority	Control Baseline
AU-3	Content of Audit Records	P1	AU-3 (1)

The State of Montana maintains 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)
- User or subject associated with the event

Control Number	Control Name	Priority	Control Baseline
AU-4	Audit Storage Capacity	P1	AU-4

The State of Montana maintains audit records on a storage area that allows flexibility in the size of the information collected.

Control Number	Control Name	Priority	Control Baseline
AU-5	Response to Audit Processing Failures	P1	AU-5

The audit system sends alerts to system owners for audit processing failures. Administrators of the audit system will stop audit record generation if a failure occurs.

Control Number	Control Name	Priority	Control Baseline
AU-6	Audit Review, Analysis, and Reporting	P1	AU-6 (1) (3)

The State of Montana (SITSD through its SIEM product) reviews audit records on a monthly basis unless otherwise specified in the audit procedure. 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.

Any security violations must be reported to the SITSD Service Desk.

Servers must be periodically audited for compliance with the existing security policies. These audits must be performed at least once a quarter.

Control Number	Control Name	Priority	Control Baseline
AU-7	Audit Reduction and Report Generation	P2	AU-7 (1)

State Information systems are able to process audit records based on selected event criteria (e.g., SIEM product).

Control Number	Control Name	Priority	Control Baseline
AU-8	Time Stamps	P1	AU-8 (1)

State information systems generate time stamps for audit records using the external naval clock time process. (Synchronization: The interval for checking time is 10 minutes. There are three NTP sources in the list. The default behavior is that all of the desktops that are joined to the Enterprise Active Directory will get their time from the Active Directory domain controllers, which in turn get the time from the NTP sources. As long as someone has not changed this default behavior on desktops or removed it from the Enterprise Active Directory, then the time stamps will be consistent.)

Control Number	Control Name	Priority	Control Baseline
AU-9	Protection of Audit Information	P1	AU-9 (4)

Access to audit information and tools is limited to those whose job duties require access or those staff who are performing the audit function.

Auditing functions will be administered by designated Agency Security Officers unless otherwise documented.

Control Number	Control Name	Priority	Control Baseline
AU-11	Audit Record Retention	P3	AU-11

Audit records are maintained for minimum of 6 years to meet regulatory requirements. (Check on records management requirement, SoS)

Control Number	Control Name	Priority	Control Baseline
AU-12	Audit Generation	P1	AU-12

Audit reports for State information systems are generated for events defined in AU-2 with content defined in AU-3.

FAMILY/Category: Certification, Accreditation, and Security Assessments (CA)

Control Number	Control Name	Priority	Control Baseline
CA-1	Security Assessment & Authorization Policy & Procedures	P1	CA-1

The State of Montana reviews and updates Security Assessment and Authorization policies and procedures within two years of last review.

Control Number	Control Name	Priority	Control Baseline
CA-2	Security Assessments	P2	CA-2 (1)

The State of Montana uses a NIST based risk assessment process and template. This process includes security controls and their effectiveness, as well as the assessment environment, team, and roles and responsibilities. The State of Montana creates a risk assessment for each information system and updates as major changes occur.

Control Number	Control Name	Priority	Control Baseline
CA-3	System Interconnections	P2	CA-3 (5)

The State requires an Interconnection Security Agreement for all information systems directly connecting to external systems. Each State information system has a security plan that outlines the connections with other information systems. The State of Montana employs a permit-by-documented request (exception) policy for allowing agency and other information systems to connect to external information systems.

Control Number	Control Name	Priority	Control Baseline
CA-5	Plan of Action and Milestones	P3	CA-5

The system owner tracks all mitigation efforts related to gaps discovered from the risk assessment for each State information system through a plan of action and milestones process. The actions are reviewed and updated quarterly.

Control Number	Control Name	Priority	Control Baseline
CA-6	Security Authorization	P3	CA-6

The authorized senior level manager reviews and approves all new information systems and major updates before they go into production.

Control Number	Control Name	Priority	Control Baseline
CA-7	Continuous Monitoring	P3	CA-7

The State Montana has established a continuous monitoring strategy and conducts continuous monitoring of State information systems on a monthly basis. The State provides information regarding current gaps in security to appropriate management officials as a result of this monitoring process.

Control Number	Control Name	Priority	Control Baseline
CA-9	Internal System Connections	P1	CA-9

The State of Montana documents all internal connections for the information system.

FAMILY/Category: Configuration Management (CM)

Control Number	Control Name	Priority	Control Baseline
CM-1	Configuration Management Policy & Procedures	P1	CM-1

The State of Montana reviews and updates Configuration Management policies and procedures within two years of last review.

Control Number	Control Name	Priority	Control Baseline
CM-2	Baseline Configuration	P1	CM-2 (1) (3) (7)

The State of Montana maintains a current baseline configuration of each State information system. These configurations are reviewed and updated on a bi-annual basis or as needed. Older versions of baseline configurations are maintained for rollback support.

Control Number	Control Name	Priority	Control Baseline
CM-3	Configuration Change Control	P1	CM-3

The State of Montana has a formalized Change Management system. This system includes the following:

a. Identifies the types of changes that need to be documented in the tool
b. Has an approval process that includes security review
c. Documents approved changes
d. Retains records of changes and includes a review process
e. Auditing of change activities
f. Coordinates and provides oversight for configuration change control activities
g. Users will be notified when the network and/or file server will be down for scheduled maintenance according to the following: All employees will be notified at least one week in advance that the computer system will not be available during scheduled maintenance. Included in this notice will be the estimated time of outage and scope of maintenance. Unscheduled maintenance will be handled on a case-by-case basis and when not an emergency, users should be given as much notice as possible.
h. Promote awareness of agency IT changes to systems though change notification. State agencies should submit a Change Notification for all IT changes that have a moderate risk of having a significant impact on multiple state agencies.
    - Change notifications will be submitted using the **Enterprise Change Notification form** located on the SITSD Customer Service Portal at least seven days prior to the scheduled change.
    - The notification will include:
        - Description of the Change (title), Agency Point of Contact (name, phone number), Change Type (Routine, Minor, Major, Urgent), Impact, Urgency, Planned Start Time (date, time), Planned End Time (date, time), Technical Description (work being performed), and Customer Impact (what will happen).
    - The SITSD Change Manager will post notifications to the Forward Schedule of Changes located on the SITSD Service Desk website
    - Agency Change Notifications will be reviewed and discussed weekly at the Wednesday Change Advisory Board (CAB) meeting. Meeting information can be found at: http://mine.mt.gov/it/changemanagement/default.mcpx

- For Urgent Changes – (Immediate change is required to resolve or avoid a major incident) Agencies should notify the SITSD Service Desk ASAP so proper notification can be sent to all agencies impacted.

i. A way to document changes, approve them, hold until approved, and document the completion of the change to the information system
j. Includes a process to test, validate, and document changes before they are implemented

Control Number	Control Name	Priority	Control Baseline
CM-4	Security Impact Analysis	P2	CM-4 (3)

The appropriate security staff review all changes before they take place. The State of Montana tests, validates, and documents changes to information systems before implementation to determine potential security impacts.

Control Number	Control Name	Priority	Control Baseline
CM-5	Access Restrictions for Change	P1	CM-5

The appropriate staff define, document, approve, and enforce physical and logical access restrictions associated with changes to State information systems.

Control Number	Control Name	Priority	Control Baseline
CM-6	Configuration Settings	P1	CM-6

The State of Montana has mandatory configuration settings for each information system and maintains these as systems are moved to production. The State also documents and approves any exceptions to configuration settings before implementation.

Control Number	Control Name	Priority	Control Baseline
CM-7	Least Functionality	P1	CM-7 (1) (2) (4)

Each State information system is reviewed and functions, ports, protocols, and/or services are limited where applicable. SITSD maintains an enterprise list of software (exceptions, white and black list). Inventory of systems is conducted annually and reviewed for any unauthorized software use. Unauthorized software is removed.

Control Number	Control Name	Priority	Control Baseline
CM-8	Information System Component Inventory	P1	CM-8 (1) (3) (5)

The State of Montana maintains an inventory of information system components. Inventory of systems is conducted annually and reviewed for any unauthorized components. Unauthorized components are removed.

Control Number	Control Name	Priority	Control Baseline
CM-9	Configuration Management Plan	P1	CM-9

The State of Montana has a configuration management plan.

Control Number	Control Name	Priority	Control Baseline
CM-10	SOFTWARE USAGE RESTRICTIONS	P1	CM-10

The State of Montana has a Software Asset Management Office that assists with software agreements, contracts, and compliance audits.

Control Number	Control Name	Priority	Control Baseline
CM-11	USER-INSTALLED SOFTWARE	P1	CM-11

The State of Montana only allows software to be installed by authorized staff. Software installation is established through procedures and monitored by appropriate staff.

FAMILY/Category: Contingency Planning (CP)

Control Number	Control Name	Priority	Control Baseline
CP-1	Contingency Planning Policy and Procedures	P1	CP-1

The State of Montana reviews and updates Contingency Planning policies and procedures within two years of last review.

Control Number	Control Name	Priority	Control Baseline
CP-2	Contingency Plan	P1	CP-2 (1) (3) (8)

The State of Montana:

a. Implements contingency planning through the state continuity of government program.
b. Distributes copies of the contingency plan to key contingency personnel of the State information system;
c. Coordinates contingency planning activities with incident handling activities;
d. Reviews the contingency plan for State information systems annually;
e. Revises the contingency plan to address changes to State governance, information system, or environment of operation and problems encountered during contingency plan implementation, execution, or testing; and
f. Communicates contingency plan changes to key contingency personnel.

The State has an overall contingency plan as well as an individual plan for each business unit. These plans outline the following:

- Essential missions and business functions and associated contingency requirements
- Recovery objectives, restoration priorities, and metrics
- Roles, responsibilities, and assigned individuals with contact information
- Maintaining essential missions and business functions despite disruption, compromise, or failure

The State plans for the resumption of essential missions and business functions within the recovery time identified within the contingency plan.

The State also identifies critical information system assets supporting essential missions and business functions.

Control Number	Control Name	Priority	Control Baseline
CP-3	Contingency Training	P2	CP-3

The State of Montana conducts appropriate training through the state continuity program.

Control Number	Control Name	Priority	Control Baseline
CP-4	Contingency Plan Testing	P2	CP-4 (1)

The State of Montana conducts appropriate contingency plan testing through the state continuity program.

Control Number	Control Name	Priority	Control Baseline
CP-6	Alternate Storage Site	P1	CP-6 (1) (3)

The State of Montana requires that an offsite storage site be in place and used for essential business functions.

Control Number	Control Name	Priority	Control Baseline
CP-7	Alternate Processing Site	P1	CP-7 (1) (2) (3)

The State of Montana requires that an alternative processing site be in place and used for essential business functions.

Control Number	Control Name	Priority	Control Baseline
CP-8	Telecommunications Services	P1	CP-8 (1) (2)

The State of Montana has alternate telecommunication services for essential mission and business functions at primary and alternate processing and storage sites.

The State-provided Internet, Intranet and related services are to be used for:

- the conduct of state and local government business and delivery of government services;
- transmitting and sharing of information among governmental, research, and educational organizations;
- supporting open research and education in and between national and international research and instructional institutions;
- communicating and exchanging professional information;
- encouraging debate of issues in a specific field of expertise;
- applying for or administering grants or contracts;
- announcing requests for proposals and bids;
- announcing new services for use in research or instruction; and
- conducting other appropriate State business.

The State-provided Internet, Intranet and related services are not to be used for:

a. "for-profit" activities,
b. "non-profit" or public, professional or service organization activities that aren't related to an employee's job duties, or
c. for extensive use for private, recreational, or personal activities. Employees should not have expectations of privacy for Internet use. Agency System Administrators, management, and Department of Administration personnel can monitor Internet usage for planning and managing network resources, performance, troubleshooting purposes, or if abuses are suspected. Employees must follow all other state policies when using the state provided Internet service. See section AU-1 (within this document) User Responsibilities for additional information regarding the use of state computer resources.

Each agency must have a clear policy on their business use of the Internet, intranet and related services. The policy should detail the permissible and non-permissible uses of the Internet, intranet and related services for their agency business use.

Internet filtering (or blocking) of individual sites or general classes of sites will be instituted for the following reasons: SITSD management can request an Internet site or class of sites be blocked based on an analysis of Internet site access for the following reasons:

a. network performance

b. 2) an apparent violation of existing state or federal law or policy, or
c. 3) security risks.

Sites filtered will be those sites determined to not be needed by the majority of State employees to perform their job duties.

Agencies may request Internet access to blocked sites by individual users, individual Internet sites or categories of Internet sites. Agencies may request access to filter reports. The following steps will be taken to request and implement the allow rule:

a. The Agency Head will request Internet site access using the SITSD Filter Request Form
b. The Agency Head will sign the form and submit it to the SITSD Service Desk. Electronic submission of requests will be accepted.
    - A current list of Internet sites filtered is contained in Appendix C - Blocked Internet Sites. The sites or classes of sites filtered, is subject to change at any time. SITSD will notify users of the state's Internet services prior to the implementation of a filter, unless it is deemed to be an emergency.
    - Agencies that have particular devices that need access to blocked sites can request that access be provided specifically to them. Agency requests must be received from the agency head. The request should be directed to the SITSD Service Desk.

Reporting of Internet access activity may be provided for the following reasons:

- Capacity Management. SITSD will analyze Internet traffic to ensure there is adequate bandwidth to meet user needs, including adequate response times and within budgeted costs of providing the Internet services. SITSD staff, during the course of their analysis, will report any access to a site or class of sites that does not appear to be work related and that is of sufficient volume that may be a potential capacity issue to SITSD management.
- Agency Request. Agencies can request a report of Internet sites accessed by an employee(s) of the agency. Agency requests must be in writing from the agency head using the form entitled Request for Agency Communications Records. The request should be directed to the SITSD Service Desk.
- Public Request. Requests for Internet access records of an individual employee by the public will not be honored without the approval of agency head.
- Involvement of Law Enforcement. A request from law enforcement for Internet access records cannot be honored without the appropriate court order (search warrant, etc.). This does not preclude SITSD or any other agency from contacting law enforcement as part of an investigation initiated by the agency. Agency legal counsel should be consulted whenever a court order is served or an investigation involves contact with law enforcement.

Control Number	Control Name	Priority	Control Baseline
CP-9	Information System Backup	P1	CP-9 (1)

The State of Montana conducts backups of user-level and system-level information contained in the information system as defined by the data owner. Documentation is reviewed and tested annually.

Each agency must have a written backup plan including a backup schedule, backup process and a list of mission critical applications. The backup plan must be reviewed annually and periodically tested by the agency. Each agency must maintain a notification list of designated staff to be contacted in an emergency. A copy of this list must be kept in a secure location, such as with off-site backups, and be readily accessible in case of an emergency. Mission critical data should be backed up, regardless of where it resides. On a daily basis at least one backup must be stored off-site.

Control Number	Control Name	Priority	Control Baseline
CP-10	Information System Recovery and Reconstitution	P1	CP-10 (2)

The State of Montana provides for the recovery and reconstitution of systems to a known state.

FAMILY/Category: Identification and Authentication (IA)

Control Number	Control Name	Priority	Control Baseline
IA-1	Identification and Authentication Policy and Procedures	P1	IA-1

The State of Montana reviews and updates Identification and Authentication policies and procedures within two years of last review.

Each Agency shall ensure that an organization structure is in place to:

1. assign information security responsibilities;
2. perform Identification and Authentication for Information Systems;
3. allocate adequate resources to implement Identification and Authentication controls; **4.** develop processes and procedures to measure compliance with this Standard; and
5. establish and evaluate performance measures to assess implementation of this Standard and subordinate procedures.

Control Number	Control Name	Priority	Control Baseline
IA-2	Identification and Authentication (Organizational Users)	P1	IA-2 (1) (2) (3) (8) (11) (12) (13)

The State of Montana uniquely identifies and authenticates users to its information systems. The use of multifactor authentication is required for any account(s) that has evaluated rights.

Evaluated level access given to employees must be approved by the Agency Security Officer. Employees having userIDs with evaluated privileges will be documented including the need for evaluated access.

Control Number	Control Name	Priority	Control Baseline
IA-3	Device Identification and Authentication	P1	IA-3

The State of Montana network uniquely identifies and authenticates all network attached devices compatible with the 802.1X protocol before establishing a network connection.

SITSD will assign IP addresses for authorized users of the state network. Agencies will use a private addressing scheme to provide additional security for network devices.

Control Number	Control Name	Priority	Control Baseline
IA-4	Identifier Management	P1	IA-4

The State of Montana manages information system identifiers (UserID) by receiving authorization from an authorized manager. Identifiers cannot be reused and must be disabled if not used for ninety (90) days.

Control Number	Control Name	Priority	Control Baseline
IA-5	Authenticator Management	P1	IA-5 (1) (2) (3) (11)

The State of Montana manages UserIDs to State information systems according to the following:

- Requiring a password that has a minimum of 8 characters that contains lower case and upper case letters and numbers.
- By following agency developed documented provisioning and de-provisioning process
- Requiring the change of password upon first login
- Forcing password changes every 60 days
- Enforcing non reuse of UserIDs
- Encryption of passwords in storage and transmission
- Prohibiting password reuse for six (6) generations
- Prohibiting the use of script files that contain a userID or password
- User-names must not be shared
- User only having one simultaneous connection on the network. Agency Security Contacts should document exceptions to simultaneous connections if they are needed
- Passwords must not be written down where they can be found by unauthorized personnel
- If a user changes work positions in an agency, their access rights must be reviewed and changed to match the new job position
- user rights should be reviewed annually

For systems using certificate-based authentication, the State of Montana requires the following:

- Validation of certificates
- Mapping the identity to the user account

Any information system that uses hardware token-based authentication employs mechanisms that satisfy Public Key Infrastructure (PKI) requirements.

Control Number	Control Name	Priority	Control Baseline
IA-6	Authenticator Feedback	P1	IA-6

The State of Montana's information systems obscure feedback of authentication information during the authentication process to protect the information from possible exploitation/use by unauthorized individuals.

Control Number	Control Name	Priority	Control Baseline
IA-7	Cryptographic Module Authentication	P1	IA-7

The State of Montana's information systems use mechanisms with sensitive information for authentication to a cryptographic module that meets the requirements of applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance for such authentication.

The standard for data encryption is the Advanced Encryption Standard 256bit or higher (AES 256-bit).

Control Number	Control Name	Priority	Control Baseline
IA-8	Identification and Authentication (Non-Organizational Users)	P1	IA-8 (1) (2) (3) (4)

The State of Montana's information systems uniquely identify and authenticate non-organizational users. The State of Montana uses a federated identity mechanism that allows authentication to some external platforms. This same technology also allows some external authentication to select services.

E-Pass - All websites and eGovernment services will use the State of Montana Electronic Payment Processing Portal for online electronic payment processing. An eGovernment service is an application or series of applications, accessed from the Internet that provides a specific service to a citizen or business. The application(s) are interactive (e.g. submitting a search for information and having results returned) and/or transactional (e.g. and exchange of goods or services).

FAMILY/Category: Incident Response (IR)

Control Number	Control Name	Priority	Control Baseline
IR-1	Incident Response Policy and Procedures	P1	IR-1

The State of Montana reviews and updates Incident Response policies and procedures within two years of last review.

Each agency shall develop and implement an ***incident management program,*** establishing ***general requirements*** within an Incident Management Standard(s) that:

a. Implement the lowest level of incident response standards and controls based upon NIST recommended Security Controls for Federal Information Systems (latest revision), Annex 1, Low-Impact Baseline incident response (IR) family
b. Implements Incident Management standards and procedure(s).
c. Assign information system security responsibilities;
d. **4.** Allocates adequate resources to respond quickly and effectively when information systems are breached.
e. **5.** Invokes their Incident Management procedure(s) for each declared incident.
f. **6.** Reviews the Incident Management program, process and procedure(s) annually to measure compliance with Appendix A incident response (IR) family and implement authorized changes to policy, standard(s), or procedure(s).
g. **7.** Integrates Incident Management plans, standards and procedures with operational and information requirements of the common and central incident management function provided by the Department of Administration.

Control Number	Control Name	Priority	Control Baseline
IR-2	Incident Response Training	P2	IR-2

The State of Montana trains personnel in their incident response roles and responsibilities on an annual basis.

Control Number	Control Name	Priority	Control Baseline
IR-3	Incident Response Testing	P2	IR-3 (2)

The State of Montana tests and/or exercises the incident response capability for the information system annually using designed table top 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.

Control Number	Control Name	Priority	Control Baseline
IR-4	Incident Handling	P1	IR-4 (1)

The State of Montana:

- Implements an incident handling capability for security incidents that includes preparation, detection and analysis, containment, eradication, and recovery;
- Coordinates incident handling activities with contingency planning activities; and
- Incorporates lessons learned from ongoing incident handling activities into incident response procedures, training, and testing/exercises, and implements the resulting changes accordingly.

Control Number	Control Name	Priority	Control Baseline
IR-5	Incident Monitoring	P1	IR-5

The State of Montana tracks and documents information system security incidents.

Control Number	Control Name	Priority	Control Baseline
IR-6	Incident Reporting	P1	IR-6 (1)

The State of Montana requires personnel to report suspected security incidents to the Service Desk within 24 hours of occurrence. SITSD reports enterprise security incident information to Executive staff, the Information Technology Managers Council, Information Security Managers Group, and the Legislative Audit Division on a monthly basis.
Incident records are maintained for minimum of 6 years to meet regulatory requirements
Report incidents involving Sensitive Data in their custody as follows:

- Immediately report loss or theft of Sensitive Data to appropriate law enforcement agencies.
- As soon as practical report loss, theft, or unauthorized access of Sensitive Data or security-related incidents to a supervisor, Attorney General and the State CIO.
- Document the details of any loss, theft, unauthorized access of portable device or portable storage, or security-related incident; and deliver the document to the State CIO within five business days.

Any person aware of an unreported loss, theft or compromise of Sensitive Data shall make a report to their supervisor, Attorney General and the State CIO as soon as practical.

Control Number	Control Name	Priority	Control Baseline
IR-7	Incident Response Assistance	P1	IR-7 (1)

The SITSD Service Desk and Security Office provide an incident response support service that provides advice and assistance for handling security incidents. The State Risk Management and Tort Claims Division also provides support for data incidents.

Control Number	Control Name	Priority	Control Baseline
IR-8	Incident Response Plan	P1	IR-8

The State of Montana has an ISIRT (Information Systems Incident Response Team) Manual that:

- Provides a roadmap for implementing its incident response capability
- Describes the structure and organization of the incident response capability
- Provides a high level approach for how the incident response capability fits into State of Montana processes
- Meets the requirements of mission, size, structure, and functions of the State of Montana
- Defines reportable incidents
- Provides metrics for measuring the incident response capability for the State of Montana
- Defines the resources and management support needed to effectively maintain and mature an incident response capability
- Is reviewed and approved by management

The State of Montana reviews and updates the ISIRT on a quarterly and an as needed basis and distributes updated information to the ISIRT members as revisions are completed.

FAMILY/Category: Maintenance (MA)

Control Number	Control Name	Priority	Control Baseline
MA-1	System Maintenance Policy and Procedures	P1	MA-1

The State of Montana reviews and updates System Maintenance policies and procedures within two years of last review.

Control Number	Control Name	Priority	Control Baseline
MA-2	Controlled Maintenance	P2	MA-2

The State of Montana uses a formalized change management process that includes maintenance of equipment. Performance of maintenance on major equipment that contains sensitive information occurs on-site and security checks are performed after maintenance is completed.

Control Number	Control Name	Priority	Control Baseline
MA-3	Maintenance Tools	P2	MA-3 (1) (2)

The State of Montana approves, controls, monitors the use of, and maintains on an ongoing basis, information system maintenance tools. Tools are checked as they enter a secured data center facility. All media is checked for virus or malicious code before it is used on an information system.

Control Number	Control Name	Priority	Control Baseline
MA-4	Non-Local Maintenance	P1	MA-4(2)

The State of Montana:

a. Authorizes, monitors, and controls non-local maintenance and diagnostic activities;
b. Allows the use of non-local maintenance and diagnostic tools only as consistent with organizational policy and documented in the system operational security plan for the information system;
c. Employs strong identification and authentication techniques in the establishment of non-local maintenance and diagnostic sessions;
d. Maintains records for non-local maintenance and diagnostic activities; and
e. Terminates all sessions and network connections when non-local maintenance is completed.

Control Number	Control Name	Priority	Control Baseline
MA-5	Maintenance Personnel	P1	MA-5

The State of Montana:

a. Has an established process for maintenance personnel authorization and maintains a current list of authorized maintenance organizations or personnel; and
b. Ensures that personnel performing maintenance on an information system that contains sensitive information must have had a background check.

The State of Montana ensures that cleared foreign nationals performing maintenance and diagnostic activities on information systems owned by the State of Montana, have proper Agreements in place with each foreign national.

Control Number	Control Name	Priority	Control Baseline
MA-6	Timely Maintenance	P1	MA-6

The State of Montana obtains maintenance support and/or spare parts for critical network and enterprise server infrastructure, IPS/IDS, and web-content filtering within twenty-four (24) hours.

FAMILY/Category: Media Protection (MP)

Control Number	Control Name	Priority	Control Baseline
MP-1	Media Protection Policy and Procedures	P1	MP-1

The State of Montana reviews and updates Media Protection policies and procedures within two years of last review.

Control Number	Control Name	Priority	Control Baseline
MP-2	Media Access	P1	MP-2

The State of Montana restricts 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).

Control Number	Control Name	Priority	Control Baseline
MP-3	Media Marking	P1	MP-3

The State of Montana marks Confidential and For Official Use Only, in accordance with organizational policies and procedures, on removable information system media and information system output indicating the distribution limitations, handling caveats, and applicable security markings (if any) of the information. If the information remains in a physically secured area it is not required to be marked.

Control Number	Control Name	Priority	Control Baseline
MP-4	Media Storage	P1	MP-4

The State of Montana:

a. Physically controls and securely stores failed or retired hard drives and tape media that contains sensitive information within designated secure areas within facilities using physical control restrictions;
b. Protects sensitive information system media until the media are destroyed or sanitized using approved equipment, techniques, and procedures.
   Sensitive Data shall:
   - Not be used or stored outside of State offices unless there is a business requirement approved by the department head.
   - Only be stored on State-owned portable devices and portable storage if there is a business requirement.
   - Be encrypted on portable devices and portable storage.
   - Not be transferred to non-State-owned portable devices or portable storage unless there is a business requirement.

Control Number	Control Name	Priority	Control Baseline
MP-5	Media Transport	P1	MP-5 (4)

The State of Montana:

a. Protects and controls sensitive information system media during transport outside of controlled areas using authorized personnel and secured transport.
b. Maintains accountability for sensitive information system media during transport outside of controlled areas.
c. Restricts the activities associated with transport of such media to authorized personnel.
d. Documents activities associated with the transport of sensitive information system media.
e. Employs cryptographic mechanisms to protect the confidentiality and integrity of sensitive information stored on digital media during transport outside of controlled areas.
   Sensitive Data shall:
   - Not be copied or removed from Secured Storage Environments unless there is a business requirement.
   - Not be transmitted via non State-owned networks unless approved transmission protocols and encryption techniques are utilized.
   - Not be transported outside of the United States on portable devices and portable storage.
     Each agency shall:
     - Document business requirements for Sensitive Data. Documentation shall be available to appropriate agency IT staff and management.
     - Maintain a documented audit trail (including a date/time record of significant changes) and inventory of:
       - who has what Sensitive Data
         - Ensure the portable device has an asset/property tag containing appropriate contact information.
         - Label all portable device components and portable storage for individual identification.
         - Do not leave portable devices and portable storage unattended in non- secured areas.
         - Do not leave the portable device or portable storage in an unlocked vehicle; place the devices and storage in a locked trunk or out of plain sight in the locked passenger compartment.
         - Store portable devices and portable storage in a safe when staying in a hotel.
         - Monitor the whereabouts of the portable device and portable storage as they pass through airport security checkpoints and retrieve them as soon as
         - Possible to minimize the risk of loss or theft.

        - Confer with departmental technical support or the State CIO for specific technology selections and implementation procedures for encryption of data.
    - what is the business requirement
    - what portable devices or storage are used
  - When traveling outside of the United States with portable devices or portable storage:
    - Prior to travel remove any Sensitive Data from the portable devices and portable storage.
    - During travel do not store Sensitive Data on portable devices and portable storage.

Control Number	Control Name	Priority	Control Baseline
MP-6	Media Sanitization	P1	MP-6

The State of Montana:

a. Sanitizes sensitive information system media (both digital and non-digital) prior to disposal, release of organizational control, or reuse; and
b. Employs sanitization mechanisms with strength and integrity commensurate with the classification or sensitivity of the information.
c. All computer storage devices must be sanitized prior to disposal, regardless of where the agency chooses to dispose of them.
d. All agency data and software programs must be removed from the hard drive prior to its disposal; or, alternatively, the hard drive must be destroyed.
e. To remove data and software, agency IT personnel should use a Department of Defense (DoD) sanitation program that will effectively sanitize the hard drive.
f. Employed sanitation mechanisms (strength and integrity) must be commensurate with the classification and sensitivity of the information.
g. If the data storage device cannot be put through this process because it is not functional, the device must be physically destroyed.
h. All removable storage media must be physically destroyed.
i. Agency directors are responsible for maintaining documentation on all electronic data storage devices (e.g., PCs, laptops, servers, portable devices) that have been either destroyed or sanitized. These records must be retained by the agency for six years.

The disposal records shall contain the following information:

- Device identification (vendor serial number or Dell service tag number)
- Date of cleaning
- Employee name performing cleaning
- Method of cleaning
- Destination of device (surplus, landfill, etc)
- Disposing Agency

Control Number	Control Name	Priority	Control Baseline
MP-7	Media Use	P1	MP-7 (1)

The State of Montana prohibits the use of portable storage devices in organizational information systems when such devices have no identifiable owner.

FAMILY/Category: Physical and Environmental Protection (PE)

Control Number	Control Name	Priority	Control Baseline
PE-1	Physical and Environmental Protection Policy and Procedures	P1	PE-1

The State of Montana reviews and updates Physical and Environmental Protection policies and procedures within two years of last review.

Control Number	Control Name	Priority	Control Baseline
PE-2	Physical Access Authorizations	P1	PE-2

The State of Montana:

a. Develops and keeps current a list of personnel with authorized access to the facilities where information systems reside;
b. Issues authorization credentials;
c. Reviews and approves the access list and authorization credentials on a monthly basis, removing from the access list personnel no longer requiring access.

Control Number	Control Name	Priority	Control Baseline
PE-3	Physical Access Control	P1	PE-3

The State of Montana:

a. Enforces physical access authorizations for all physical access points where the information system resides;
b. Verifies individual access authorizations before granting access to facilities;
c. Controls entry to facilities containing the information system using physical access controls;
d. Controls access to areas officially designated as publicly accessible in accordance with the organization's assessment of risk;
e. Secures keys, combinations, and other physical access devices;
f. Inventories physical access devices annually; and
g. Changes combinations and keys when keys are lost, combinations are compromised, or individuals are transferred or terminated.

Only personnel authorized to operate a server will have access to the physical area where the server resides. Keys and/or other security devices must be used to secure the physical area and a list of all authorized personnel maintained. In areas with highly secure servers, cleaning and maintenance personnel must be supervised by an authorized user while they are working in the area.

Access to network equipment such as routers, switches, firewalls, patch panels, gateways, communication servers and the like must be controlled the same as servers. Physical access must be restricted to prevent tampering or accidental disruption of service. Servers and other network equipment must be kept in a locked environment, only accessible by authorized systems support personnel. It is the responsibility of the agency to provide a secured area to house network equipment and servers.

Control Number	Control Name	Priority	Control Baseline
PE-4	Access Control for Transmission Medium	P1	PE-4

The State of Montana controls physical access to information system distribution and transmission lines within state facilities.

Control Number	Control Name	Priority	Control Baseline
PE-5	Access Control for Output Devices	P1	PE-5

The State of Montana controls physical access to sensitive information system output devices to prevent unauthorized individuals from obtaining the output.

Control Number	Control Name	Priority	Control Baseline
PE-6	Monitoring Physical Access	P1	PE-6 (1)

The State of Montana:

a. Monitors physical access to information systems to detect and respond to physical security incidents;
b. Reviews physical access logs monthly; and
c. Coordinates results of reviews and investigations with the state's incident response capability.

Real-time physical intrusion alarms and surveillance equipment are monitored for security incidents.

Control Number	Control Name	Priority	Control Baseline
PE-8	Visitor Access Records	P3	PE-8

The State of Montana maintains visitor access records to facilities that house sensitive information systems and reviews visitor access records monthly.

Control Number	Control Name	Priority	Control Baseline
PE-9	Power Equipment and Cabling	P1	PE-9

The State of Montana protects power equipment and power cabling for sensitive information systems from damage and destruction.

Care should be taken when positioning the computer electrical cords. They should not be positioned near a heating element, under file cabinets, or in a manner that may be a hazard for walking.

To protect data in the event of power fluctuations or outages, a surge suppressor or UPS should be used on all computers. Non-computer equipment such as heaters and fans should not share the same surge suppressor as the computer. NOTE: Most UPS's are not laser printer compatible. Be sure to read the documentation provided with your UPS.

Control Number	Control Name	Priority	Control Baseline
PE-10	Emergency Shutoff	P1	PE-10

The State of Montana:

a. Provides the capability of shutting off power to sensitive information systems or individual system components in emergency situations;
b. Places emergency shutoff switches or devices in appropriate locations within secured facilities to facilitate safe and easy access for personnel; and
c. Protects emergency power shutoff capability from unauthorized activation.

Control Number	Control Name	Priority	Control Baseline
PE-11	Emergency Power	P1	PE-11

The State of Montana provides a short-term uninterruptible power supply to facilitate an orderly shutdown of information systems in the event of a primary power source loss.

Control Number	Control Name	Priority	Control Baseline
PE-12	Emergency Lighting	P1	PE-12

The State of Montana employs and maintains 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.

Control Number	Control Name	Priority	Control Baseline
PE-13	Fire Protection	P1	PE-13 (3)

The State of Montana:

a. Employs and maintains fire suppression and detection systems for sensitive information systems that are supported by an independent energy source.
b. Employs fire detection systems for sensitive information systems that activate automatically and notify authorized personnel and emergency responders in the event of a fire.
c. Employs fire suppression systems for sensitive information systems that provide automatic notification of any activation to State emergency responders.
d. Employs an automatic fire suppression capability for sensitive information systems for unstaffed facilities.

Control Number	Control Name	Priority	Control Baseline
PE-14	Temperature and Humidity Controls	P1	PE-14

The State of Montana:

a. Maintains temperature and humidity levels within the facilities where sensitive information systems reside at between 68-71 degrees Fahrenheit and humidity can be anywhere from 28% to 54%.
b. Monitors temperature and humidity levels 24/7.

Care should be taken when positioning a computer in the work environment. Computers should be well ventilated. They should not be put in a position that covers the vent for the fan.

Control Number	Control Name	Priority	Control Baseline
PE-15	Water Damage Protection	P1	PE-15

The State of Montana protects sensitive information systems from damage resulting from water leakage by providing master shutoff valves that are accessible, working properly, and known to key personnel.

Control Number	Control Name	Priority	Control Baseline
PE-16	Delivery and Removal	P1	PE-16

The State of Montana 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.

Control Number	Control Name	Priority	Control Baseline
PE-17	Alternate Work Site	P1	PE-17

The State of Montana:

a. Employs the same security controls and requirements in all of its facilities that contain sensitive information systems: Miles City Data Canter, Helena Data Center, Mitchell Building, IConnect, and Federal Reserve Bank Building;
b. Assesses as feasible, the effectiveness of security controls at alternate work sites; and
c. Provides a means for employees to communicate with information security personnel in case of security incidents or problems.

FAMILY/Category: Planning (PL)

Control Number	Control Name	Priority	Control Baseline
PL-1	Security Planning Policy and Procedures	P1	PL-1

The State of Montana reviews and updates Security Planning policies and procedures within two years of last review.

Control Number	Control Name	Priority	Control Baseline
PL-2	System Security Plan	P1	PL-2 (3)

The State of Montana:

a. Develops a security plan for information systems that:
   - Is consistent with enterprise architecture;
   - Explicitly defines the authorization boundary for the systems;
   - Describes the operational context of the information systems in terms of missions and business processes;
   - Provides the security categorization of the information systems including supporting rationale;
   - Describes the operational environment for the information systems;
   - Describes relationships with or connections to other information systems;
   - Provides an overview of the security requirements for the systems;
   - 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;

b. Reviews the security plans for information systems every two years or when major changes occur to the system; and

c. Updates the plan to address changes to the information system/environment of operation or problems identified during plan implementation or security control assessments.

The State of Montana plans and coordinates security-related activities affecting the information system with all affected agencies before conducting such activities in order to reduce the impact on other organizational entities.

Control Number	Control Name	Priority	Control Baseline
PL-4	Rules of Behavior	P1	PL-4 (1)

The State of Montana:

a. Establishes and makes readily available to all information system users, the rules that describe their responsibilities and expected behavior with regard to information and information system usage; and
b. Receives signed acknowledgment from users indicating that they have read, understand, and agree to abide by the rules of behavior, before authorizing access to information and the information system.

The organization includes in the rules of behavior, explicit restrictions on the use of social media/networking sites and posting information on commercial websites.

Each user of the State of Montana's computing and information resources should realize the fundamental importance of information resources and is responsible for the safe keeping of these resources. Users and system administrators must guard against abuses that disrupt or threaten the viability of all systems, including those on the State network and those on networks to which State systems are connected.

Each user is responsible for having knowledge of the State's policies concerning security and care for their computer. It is the responsibility of the State to educate its management and staff about these policies; to educate its employees about the dangers of computer abuse and its threat to the operation of the State computer network; and educate its management and staff about proper ethical behavior, acceptable computing practices, and copyright and licensing issues.

Each user of the State of Montana's computing and information resources must act responsibly. Each user is responsible for the integrity of these resources. All users of State-owned or State-leased computing systems must be knowledgeable of and adhere to agency policies, respect the rights of other users by minimizing unnecessary network traffic that might interfere with the ability of others to make effective use of this shared network resource, respect the integrity of the physical facilities and controls, and obey all federal, state, county, and local laws and ordinances.

All employees must abide by these policies, relevant laws and contractual obligations, and appropriate ethical standards. State computing facilities and UserIDs are to be used for the job-related activities for which they are assigned. State computing resources are not to be used for the following:

1. private commercial purposes,
2. non-State-related activities (including games or software that is not required for an employee's job responsibilities), or 3. non-State standard software. Exceptions can be granted by ITSD for the use of software for which a State standard exists.

B. Misuse Of Computer Resources

The following items represent, but do not fully define, misuse of computing and information resources:

1. Using computer resources to create, access, download, or disperse derogatory, racially offensive, sexually offensive, harassing, threatening, or discriminatory materials.
2. Down-loading, installing, or running security programs or utilities which reveal weaknesses in the security of the state's computer resources unless a job specifically requires it.
3. Use of computers and userIDs for which there is no authorization, or use of userIDs for purpose(s) outside of those for which they have been issued.
4. Attempting to modify, install, or remove computer equipment, software, or peripherals without proper authorization. This includes installing any non-work related software on State-owned equipment.
5. Accessing computers, computer software, computer data or information, or networks without proper authorization, regardless of whether the computer, software, data, information, or network in question is owned by the State. (That is, if you abuse the networks to which the State has access or the computers at other sites connected to those networks, the State will treat this matter as an abuse of your computing privileges.)

6. Circumventing or attempting to circumvent normal resource limits, logon procedures, and security regulations.
7. The use of computing facilities, userIDs, or computer data for purposes other than those for which they were intended or authorized.
8. Sending fraudulent email, breaking into another user's email box, or unauthorized personnel reading someone else's email without his or her permission.
9. Sending any fraudulent electronic transmission, including but not limited to fraudulent requests for confidential information, fraudulent submission of electronic purchase requisitions or journal vouchers, or fraudulent electronic authorization of purchase requisitions or journal vouchers.
10. Violating any software license agreement or copyright, including copying or redistributing copyrighted computer software, data, or reports without proper, recorded authorization. State employees must honor copyright laws regarding protected commercial software or intellectual property. Duplicating, transmitting, or using software or other electronic property not in compliance with license agreements is considered copyright infringement. State employees are not to make copies of any copyrighted materials without the full legal right to do so. Unauthorized use of copyrighted materials or another person's original writings is considered copyright infringement. Copyrighted materials belonging to others may not be transmitted by staff members on the Internet without permission. Users may download copyrighted material from the Internet, but its use must be strictly within the agreement as posted by the author or current copyright law. In addition, copyrighted agency/State information used on web sites must be clearly labeled as such.
11. Taking advantage of another user's naiveté or negligence to gain access to any userID, data, software, or file that is not your own and for which you have not received explicit authorization to access.
12. Physically interfering with other users' access to the State's computing facilities.
13. Encroaching on or disrupting others' use of the State's shared network resources by creating unnecessary network traffic (for example, playing games or sending excessive messages); wasting computer time, connect time, disk space, or other resources; modifying system facilities, operating systems, or disk partitions without authorization; attempting to crash or tie up a State computer; damaging or vandalizing State computing facilities, equipment, software, or computer files).
14. Disclosing or removing proprietary information, software, printed output or magnetic media without the explicit permission of the owner.
15. Reading other users' data, information, files, or programs on a display screen, as printed output, or via electronic means, without the owner's explicit permission.
16. Knowingly transferring or allowing to be transferred to, from or within the agency, textual or graphical material commonly considered to be child pornography or obscene as defined in 45-8-201(2), MCA.

Rules of System Usage

All State employees or contractors with the State who have access to the Internet, email, or other online services, will sign a consent form indicating that they have knowledge of the state's policies and procedures in regards to the use of state computing resources. Privacy in using the state's computer systems is not guaranteed. Therefore, employees should not have any expectations of privacy when using the Internet, email, or other computer services. The following is an example consent form that agencies can use for employees and contractors. Both employees and contractors shall read and sign a consent form every year.

Rules of System Usage Sample Acknowledgement Form

I _____ have read the (***Add Agency***) policies and procedures regarding the use of information systems and I agree to comply with all terms and conditions. I agree that all information system activity conducted while doing (***Add Agency***) business and being conducted with (***Add Agency***) resources is the property of the State of Montana. I understand that any information system to which I have access, can only be used for its intended purpose. I also agree to avoid the disclosure of any protected data to which I have access.

I understand that (***Add Agency***)/SITSD reserves the right to monitor and log all information system activity including email and Internet use, with or without notice, and therefore I should have no expectations of privacy in the use of these resources.

If my position requires a background check, I understand that the results of this background check can affect my employment.

_____ Yes, this position requires a background check
_____ No, this position does not require a background check.

Signed _____

Position Title _____ Position Number _____

Date _____

*NOTE: This form will be signed by each (**Add Agency**) employee on an annual basis.*

Control Number	Control Name	Priority	Control Baseline
PL-8	INFORMATION SECURITY ARCHITECTURE	P1	PL-8

The State of Montana:

a. Develops 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; and
   - Describes any information security assumptions about, and dependencies on, external services;

b. Reviews and updates the information security architecture every two years to reflect updates in the enterprise architecture; and

c. Ensures that planned information security architecture changes are reflected in the operational security plan, the security Concept of Operations, and organizational procurements/acquisitions.

FAMILY/Category: Personnel Security (PS)

Control Number	Control Name	Priority	Control Baseline
PS-1	Personnel Security Policy and Procedures	P1	PS-1

The State of Montana reviews and updates Personnel Security policies and procedures within two years of last review.

Control Number	Control Name	Priority	Control Baseline
PS-2	Position Risk Designation	P1	PS-2

The State of Montana:

a. Assigns a risk designation to all positions;

b. Establishes screening criteria for individuals filling those positions; and

c. Reviews and revises position risk designations every two years.

Control Number	Control Name	Priority	Control Baseline
PS-3	Personnel Screening	P1	PS-3

The State of Montana:

a. Screens individuals prior to authorizing access to information systems; and

b. Rescreens individuals according to the following conditions: job-transfer/hire into a position that requires additional security access to raised floor areas or positions that are housed at secured data center facilities; as required by state policy (every 3 years).

Control Number	Control Name	Priority	Control Baseline
PS-4	Personnel Termination	P2	PS-4

The State of Montana, upon termination of individual employment:

a. Terminates all information system access;

b. Conducts exit interviews;

c. Retrieves all security-related organizational information system-related property; and

d. Retains access to organizational information and information systems formerly controlled by terminated individual.

Control Number	Control Name	Priority	Control Baseline
PS-5	Personnel Transfer	P2	PS-5

When reassigning or transferring personnel to other positions within the State, a review of logical and physical access authorizations to information systems/facilities is performed within three business days of beginning the new position to ensure access is limited to authorized and required systems/facilities.

Control Number	Control Name	Priority	Control Baseline
PS-6	Access Agreements	P3	PS-6

The State of Montana:

a. Ensures that individuals requiring access to organizational sensitive information sign appropriate access agreements prior to being granted access; and
b. Reviews/updates the access agreements every two years.

Rules of System Usage for Users with Elevated Privileges Sample Acknowledgement Form

A. INTRODUCTION

I _____, understand that I have additional responsibilities given my elevated computer access privileges. I have received training emphasizing the effects my actions can have on all information system activity. Because of these responsibilities, I understand the need for reading and signing this Acknowledgement.

B. FEDERAL AND STATE TAX INFORMATION

I understand the following:

1. I may have access to Federal Tax Information (FTI) and State Tax information as defined in footnote 1 below.
2. That tax returns or tax information disclosed to each user can be used only for a purpose and to the extent authorized by the data manager in connection with the processing, storage, transmission and reproduction of tax returns and return information, the programming, maintenance, repair, testing, and procurement of equipment, and providing of other services for purposes of tax administration.
3. That further disclosure of any tax returns or tax information for a purpose or to an extent unauthorized by the data manager for these purposes constitutes a felony, punishable upon conviction by a fine of as much as $5,000, or imprisonment for as long as five years, or both, together with the costs of prosecution (IRC 7213).
4. That further inspection of any tax returns or tax information for a purpose or to an extent not authorized by the data manager for these purposes constitutes a misdemeanor, punishable upon conviction by a fine of as much as $1,000, or imprisonment for as long as one year, or both, together with costs of prosecution (IRC 7213A)
5. That should either unauthorized access or disclosure occur, individually I can be sued by the taxpayer and would be liable for civil damages amounting to a minimum of $1,000 for each act or the actual damages sustained by the taxpayer (whichever is greater) as well as the costs of the court action (IRC 7431).
6. That under Montana law, 15-30-303 MCA, 15-70-209 MCA, 15-70-344 MCA, 15-70-351, MCA, a user cannot disclose or disseminate information contained in a statement required under the fuel tax sections. Making an unauthorized disclosure or unauthorized inspection of information can make the person subject to the progressive disciplinary procedures set out by state law which could include termination from employment.
7. I have received awareness training and understand the policies and procedures for safeguarding FTI and the penalties for unauthorized inspection or disclosure of FTI.

C. CRIMINAL JUSTICE INFORMATION

I understand the following:

1. I may have access to criminal justice information as defined in footnote 2 below, via the state network.
2. My access to this information is limited for the purpose(s) outlined in the agreement between the State Information Technology Services Division and the government agency providing the information.
3. Criminal history information and related data are particularly sensitive and may cause great harm if misused.
4. Misuse of the system by accessing it without authorization, exceeding the authorization, using the system improperly, or using, disseminating or re-disseminating criminal justice information without authorization, may constitute a state crime, federal crime, or both.

D. OTHER CONFIDENTIAL INFORMATION

I understand that I may have access to other confidential information such as a person's first and last name, address, telephone number, email address, social security number, bank and credit card information, health information, and other unique identifying information about a person. This information is confidential and may not be used or disclosed without proper authorization from my supervisor.

I have read and understand this Acknowledgement. A violation of the above terms and conditions may result in disciplinary action up to and including termination from employment.

Signed _____
Date _____

1. **FTI (IRS Code) -** A taxpayer's identity, the nature, source, or amount of his income, payments, receipts, deductions, exemptions, credits, assets, liabilities, net worth, tax liability, tax withheld, deficiencies over assessments, or tax payments, whether the taxpayer's return was, is being, or will be examined or subject to other investigation or processing.
2. **CJIS Data -** data considered to be criminal justice in nature to include images, files, records, and intelligence information. FBI CJIS data is information derived from state or Federal CJIS systems.

Control Number	Control Name	Priority	Control Baseline
PS-7	Third-Party Personnel Security	P1	PS-7

The State of Montana:

a. Establishes personnel security requirements including security roles and responsibilities for third-party providers;
b. Documents personnel security requirements; and
c. Monitors provider compliance.

Control Number	Control Name	Priority	Control Baseline
PS-8	Personnel Sanctions	P3	PS-8

The State of Montana employs a formal sanctions process for personnel failing to comply with established information security policies and procedures.

FAMILY/Category: Risk Assessment (RA)

Control Number	Control Name	Priority	Control Baseline
RA-1	Risk Assessment Policy and Procedures	P1	RA-1

The State of Montana reviews and updates Risk Assessment policies and procedures within two years of last review.

Control Number	Control Name	Priority	Control Baseline
RA-2	Security Categorization	P1	RA-2

The State of Montana:

a. Categorizes information systems in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance;
b. Documents the security categorization results in the security plan for each information system; and
c. The authorizing official or designated representative ensures review and approval of the security categorization decision.

Control Number	Control Name	Priority	Control Baseline
RA-3	Risk Assessment	P1	RA-3

The State of Montana:

a. Conducts an assessment of risk, including 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;
b. Documents risk assessment results in risk assessment report;
c. Reviews risk assessment results annually; and
d. Updates the risk assessment annually 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.

Control Number	Control Name	Priority	Control Baseline
RA-5	Vulnerability Scanning	P1	RA-5 (1) (2) (5)

The State of Montana:

a. Scans for vulnerabilities in information systems and hosted applications annually and when new vulnerabilities potentially affecting the system/applications are identified and reported;
b. Employs vulnerability scanning tools and techniques that promote interoperability among tools and automate 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;
c. Analyzes vulnerability scan reports and results from security control assessments;
d. Remediates critical vulnerabilities within thirty (30) business days in accordance with an organizational assessment of risk; and
e. Shares information obtained from the vulnerability scanning process and security control assessments with designated personnel to help eliminate similar vulnerabilities in other information systems.

The State of Montana also employs 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.

The State of Montana authorizes privileged access for vulnerability scanning activities.

FAMILY/Category: System and Service Acquisition (SA)

Control Number	Control Name	Priority	Control Baseline
SA-1	System and Services Acquisition Policy & Procedures	P1	SA-1

The State of Montana reviews and updates System and Services Acquisition policies and procedures within two years of last review.

Control Number	Control Name	Priority	Control Baseline
SA-2	Allocation of Resources	P1	SA-2

The State of Montana:

a. Includes a determination of information security requirements for information systems in mission/business process planning;
b. Determines, documents, and allocates the resources required to protect information systems as part of its capital planning and investment control process; and
c. Establishes a discrete line item for information security in organizational programming and budgeting documentation.

Control Number	Control Name	Priority	Control Baseline
SA-3	System Development Life Cycle	P1	SA-3

The State of Montana:

a. Manages information systems using a system development life cycle methodology that includes information security considerations;
b. Defines and documents information system security roles and responsibilities throughout the system development life cycle; and
c. Identifies individuals having information system security roles and responsibilities.

Control Number	Control Name	Priority	Control Baseline
SA-4	Acquisition Process	P1	SA-4 (1) (2) (9) (10)

The State of Montana includes the following requirements and/or specifications, explicitly or by reference, in information system acquisition contracts based on an assessment of risk and in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, and standards:

a. Security functional requirements/specifications;
b. Security-related documentation requirements; and
c. Developmental and evaluation-related assurance requirements.

The State of Montana also requires in acquisition documents that vendors/contractors provide information describing the 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.

The State of Montana requires the developer of the information system, system component, or information system service to provide design and implementation information for the security controls to be employed that includes: security-relevant external system interfaces and high-level design.

The State of Montana requires the developer of the information system, system component, or information system service to identify early in the system development life cycle the functions, ports, protocols, and services intended for organizational use.

The State of Montana employs only information technology products on the FIPS 201-approved products list for Personal Identity Verification (PIV) capability implemented within organizational information systems.

Control Number	Control Name	Priority	Control Baseline
SA-5	Information System Documentation	P2	SA-5

The State of Montana:

a. Obtains, protects as required, and makes 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; and
b. Obtains, protects as required, and makes 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 in a more secure manner; and
    - User responsibilities in maintaining the security of the information and information system; and
c. Documents attempts to obtain information system documentation when such documentation is either unavailable or nonexistent.
d. Protects documentation as required in accordance with the risk management strategy.
e. Makes documentation available to authorized personnel.

Control Number	Control Name	Priority	Control Baseline
SA-8	Security Engineering Principles	P1	SA-8

The State of Montana applies information system security engineering principles in the specification, design, development, implementation, and modification of the information system.

Control Number	Control Name	Priority	Control Baseline
SA-9	External Information System Services	P1	SA-9 (2)

The State of Montana:

a. Requires that providers of external information system services comply with organizational information security requirements and employ appropriate security controls in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance;
b. Defines and documents State of Montana oversight and user roles and responsibilities with regard to external information system services; and
c. Monitors security control compliance by external service providers.

The State of Montana requires providers of information system services to identify the functions, ports, protocols, and other services required for the use of such services.

Control Number	Control Name	Priority	Control Baseline
SA-10	Developer Configuration Management	P1	SA-10

The State of Montana requires that information system developers/integrators:

a. Perform configuration management during information system design, development, implementation, and operation;
b. Manage and control changes to the information system;
c. Implement only organization-approved changes;
d. Document approved changes to the information system; and
e. Track security flaws and flaw resolution.

Control Number	Control Name	Priority	Control Baseline
SA-11	Developer Security Testing and Evaluation	P2	SA-11

The State of Montana requires that information system developers/integrators:

a. Create and implement a security test and evaluation plan;
b. Implement a verifiable flaw remediation process to correct weaknesses and deficiencies identified during the security testing and evaluation process; and
c. Document the results of the security testing/evaluation and flaw remediation processes.

FAMILY/Category: System and Communication Protection (SC)

Control Number	Control Name	Priority	Control Baseline
SC-1	System and Communications Protection	P1	SC-1

The State of Montana reviews and updates System and Communication Protection policies and procedures within two years of last review.

Control Number	Control Name	Priority	Control Baseline
SC-2	Application Partitioning	P1	SC-2

The State of Montana through access control and least privilege functions separates user functionality from information system management functionality.

Control Number	Control Name	Priority	Control Baseline
SC-4	Information in Shared Resources	P1	SC-4

The State of Montana network prevents unauthorized and unintended information transfer via shared system resources.

Control Number	Control Name	Priority	Control Baseline
SC-5	Denial of Service Protection	P1	SC-5

The State of Montana network protects against or limits the effects of the following types of denial of service attacks: consumption of computational resources, disruption of configuration information, and disruption of physical network components.

Control Number	Control Name	Priority	Control Baseline
SC-7	Boundary Protection	P1	SC-7 (3) (4) (5) (7)

The State of Montana:

a. Monitors and controls communications at the external boundary of the system and at key internal boundaries within the system; and
b. Connects to external networks or information systems only through managed interfaces consisting of boundary protection devices arranged in accordance with security architecture.

The State of Montana physically allocates publicly accessible State of Montana network components to separate sub-networks with separate physical network interfaces.

The State of Montana network prevents public access into the State of Montana's internal networks except as appropriately mediated by managed interfaces employing boundary protection devices.

The State of Montana limits 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.

The State of Montana:

a. Implements a managed interface for each external telecommunication service;
b. Establishes a traffic flow policy for each managed interface;
c. Employs security controls as needed to protect the confidentiality and integrity of the information being transmitted;
d. Documents each exception to the traffic flow policy with a supporting mission/business need and duration of that need;
e. Reviews exceptions to the traffic flow policy annually or upon request; and
f. Removes traffic flow policy exceptions that are no longer supported by an explicit mission/business need.

The State of Montana network denies network traffic by default and allows network traffic by exception (i.e., deny all, permit by exception) at managed interfaces.

The State of Montana network prevents remote devices that have established a non-remote connection with the system from communicating outside of that communications path with resources in external networks.

A separate area on the network referred to as the DMZ (Demilitarized Zone) for Internet Web and FTP Servers. All Internet web and ftp servers must reside on this area of the network. SITSD will also provide web and ftp hosting services for agencies that do not have the capabilities of moving servers to this isolated area on the network. SITSD can also house these servers in its secured data center.

Access from the trusted side of the state network to the Internet, though typically unrestricted, some restrictions may be added at the discretion of SITSD if certain protocols or traffic is determined to be a security threat.

A firewall allowing only approved externally initiated access from the Internet to the trusted side of the state network. All requests for access through the firewall will be submitted to and reviewed by SITSD, who will approve or deny the requests. Such decisions may be appealed to the State Chief Information Officer.

A firewall between an agency or portion of an agency's network and the trusted state network will be provided at the agency's expense if requested. Agency firewalls will be installed and administered by SITSD unless precluded by statutory requirements.

SITSD shall monitor all external connections to the trusted side of the state network. All external dedicated connections must use the approved method as designated in section AC-17 (within this document) Remote Access for Employees and Contractors.

SITSD shall conduct auditing of the state network including the detection and reporting of intrusion attempts performed continuously in an automated fashion. Daily review of the audit logs during the workweek. Agencies will be notified within 24 hours when their portion of the network is involved in any breaches of network security.

SITSD shall manage and install all routers, switches, firewalls, access points and any new or future telecommunications devices that support the State of Montana network.

SITSD may implement additional security measures as needed using software and/or hardware configurations for protecting the state network or ensuring secure communications. These may include encryption or filters restricting certain types of network traffic. All wireless connections to the inside (protected) portion of the network (inside) will be encrypted and authenticated. Unauthorized connections to the state network will not be permitted. Connections creating routing patterns that flood the network with unnecessary traffic are not allowed.

Agencies will cooperate to make shared sites secure and may incorporate encryption into data transmission between sites on the wide area network (WAN).

Agencies shall insure standard security checks be made on Web Servers before they are made accessible to the public.

Control Number	Control Name	Priority	Control Baseline
SC-8	Transmission Confidentiality and Integrity	P1	SC-8 (1)

The State of Montana network protects the integrity of transmitted information.

The State of Montana employs cryptographic mechanisms to recognize changes to information during transmission unless otherwise protected by alternative physical measures.

State and federal statutes provide a foundation to guarantee an appropriate level of privacy when electronic communications are used. Both users of the State of Montana's telecommunications network, and those who provide access, need a common understanding of the levels of confidentiality, security and access provided. The scope is limited to those activities associated with the "transmission" of information using the State's telecommunications network. Information transmission is facilitated through local area networks (LANs), wide area networks (WANs) and the voice network.

Such transmissions may include, but not be limited to;

electronic documents, electronic files, electronic mail, video, images and voice communications

Transmissions on the State's telecommunications network may only be intercepted (including copying and/or recording) and/or monitored (including viewing and/or listening) when such interception is in the normal course of employment responsibilities, or is regarded as necessary to providing the State's telecommunications services, or is protecting the rights and property of the State of Montana.

Transmissions may be intercepted and/or monitored to conduct mechanical checks, service quality control checks, maintenance of service quality, system security, and software license monitoring.

No telephone conversation may be recorded without the knowledge of all parties to the conversation as provided for in 45-8-213, MCA. State employees who qualify as peace officers may continue, in the course of their duties as law enforcement officers, to record conversations where one party consents (i.e., the officer) to such recordings.

No person may intentionally disclose information from intercepted and/or monitored transmissions on the State's telecommunications network except to the person for whom it is intended, to a person reasonably involved in the process of transmitting the information to the person for whom it is intended, or to another person lawfully entitled to it.

No person may use information from intercepted and/or monitored transmissions on the State's telecommunications network for any purpose other than supporting and maintaining the State's telecommunications services, or other lawful purposes. If any person is discovered misusing information from intercepted and/or monitored transmissions on the State's telecommunications network, they shall be subject to disciplinary action appropriate to the misuse, up to and including termination as administered under MOM Policy 261, Discipline Handling, Montana Operations Manual and possible civil or criminal penalties.

Control Number	Control Name	Priority	Control Baseline
SC-10	Network Disconnect	P2	SC-10

The State of Montana network terminates the network connection associated with a communications session at the end of the session or after twenty (20) minutes of inactivity.

Control Number	Control Name	Priority	Control Baseline
SC-12	Cryptographic Key Establishment and Management	P1	SC-12

The State of Montana establishes and manages cryptographic keys for required cryptography employed within information systems.

Control Number	Control Name	Priority	Control Baseline
SC-13	Cryptographic Protection	P1	SC-13

The State of Montana information systems implement required cryptographic protections using cryptographic modules that comply with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance.

Control Number	Control Name	Priority	Control Baseline
SC-15	Collaborative Computing Devices	P1	SC-15

The State of Montana network:

a. Prohibits remote activation of collaborative computing devices; and
b. Provides an explicit indication of use to users physically present at the devices.

Control Number	Control Name	Priority	Control Baseline
SC-17	Public Key Infrastructure Certificates	P1	SC-17

The State of Montana issues public key certificates under a certificate policy or obtains public key certificates under an appropriate certificate policy from an approved service provider.

Control Number	Control Name	Priority	Control Baseline
SC-18	Mobile Code	P1	SC-18

The State of Montana:

a. Defines acceptable and unacceptable mobile code and mobile code technologies;
b. Establishes usage restrictions and implementation guidance for acceptable mobile code and mobile code technologies; and
c. Authorizes, monitors, and controls the use of mobile code for information systems.

Control Number	Control Name	Priority	Control Baseline
SC-19	Voice Over Internet Protocol	P1	SC-19

The State of Montana:

a. Establishes usage restrictions and implementation guidance for Voice over Internet Protocol (VoIP) technologies based on the potential to cause damage to the State of Montana network if used maliciously; and
b. Authorizes, monitors, and controls the use of VoIP within the State of Montana network.

Control Number	Control Name	Priority	Control Baseline
SC-20	Secure Name/Address Resolution Service (Authoritative Source)	Priority 1	SC-20

The State of Montana provides an enterprise Domain Name Service (DNS) that provides additional data origin and integrity artifacts along with the authoritative data the system returns in response to name/address resolution queries.

The State of Montana DNS information system does not contain parent and child domains.

Control Number	Control Name	Priority	Control Baseline
SC-21	Secure Name /Address Resolution Service (Recursive or Caching Resolver)	P1	SC-21

The State of Montana DNS information system requests and performs data origin authentication and data integrity verification on the name/address resolution responses the system receives from authoritative sources.

Control Number	Control Name	Priority	Control Baseline
SC-22	Architecture and Provisioning for Name/Address Resolution Service	P1	SC-22

The State of Montana DNS information system that collectively provides name/address resolution services, is fault-tolerant and implements internal/external role separation.

Control Number	Control Name	Priority	Control Baseline
SC-23	Session Authenticity	P1	SC-23

The State of Montana network protects the authenticity of communications sessions.

Control Number	Control Name	Priority	Control Baseline
SC-28	Protection of Information at Rest	P1	SC-28

The State of Montana protects the confidentiality and integrity of information at rest using appropriate security technologies. Refer to the Data Classification Policy for details.

Control Number	Control Name	Priority	Control Baseline
SC-32	Information System Partitioning		

The State of Montana partitions the information system into components residing in separate physical and/or virtual domains (or environments) as deemed necessary.

Control Number	Control Name	Priority	Control Baseline
SC-39	Process Isolation	P1	SC-39

The State of Montana network system maintains a separate execution domain for each executing process where appropriate.

FAMILY/Category: System and Information Integrity (SI)

Control Number	Control Name	Priority	Control Baseline
SI-1	System and Information Integrity Policy and Procedures	P1	SI-1

The State of Montana reviews and updates System and Information Integrity policies and procedures within two years of last review.

Control Number	Control Name	Priority	Control Baseline
SI-2	Flaw Remediation (Patch Management)	P1	SI-2 (2)

The State of Montana:

a. Identifies, reports, and corrects information system flaws;
b. Tests software updates related to flaw remediation for effectiveness and potential side effects on organizational information systems before installation; and
c. Incorporates flaw remediation into state configuration management process.

The State of Montana employs automated mechanisms monthly to determine the state of information system components with regard to flaw remediation.

Control Number	Control Name	Priority	Control Baseline
SI-3	Malicious Code Protection	P1	SI-3 (1) (2)

The State of Montana:

a. Employs malicious code protection mechanisms at entry and exit points and at workstations, servers, or mobile computing devices on the network to detect and eradicate malicious code:
   - Transported by electronic mail, electronic mail attachments, web accesses, removable media, or other common means; or
   - Inserted through the exploitation of information system vulnerabilities;
b. Updates malicious code protection mechanisms (including signature definitions) daily or whenever new releases are available.
c. Configures malicious code protection mechanisms to:
   - Perform periodic scans of information systems and real-time scans of files from external sources as the files are downloaded, opened, or executed; and
   - Block malicious code, quarantine malicious code, or send alerts to administrators in response to malicious code detection
d. Addresses the receipt of false positives during malicious code detection and eradication and the resulting potential impact on the availability of the information system using incident response processes.

e. The anti-virus/malware system prevents non-privileged users from circumventing malicious code protection capabilities.
f. Virus scanning software MUST be installed, updated, and used regularly on servers, workstations, portable computers, smart phones, etc.), and any other computers being used to connect to the state's network remotely.
g. Users shall not knowingly introduce a computer virus into a state computer.
h. A user that suspects that his/her workstation has been infected by a computer virus must immediately power off the computer and call Service Desk.
i. Suspicious email messages should be forwarded to the Service Desk for investigation before they are opened. ServiceDesk@mt.gov

Firewall software must be installed, updated, and used according to standards set by SITSD on all portable computers used to connect outside of the state (Internet) firewall.

Control Number	Control Name	Priority	Control Baseline
SI-4	Information System Monitoring	P1	SI-4 (2) (4) (5)

The State of Montana:
a. Monitors events in accordance with security incident and event monitoring objectives and detects information system attacks;
b. Identifies unauthorized use of information systems;
c. Deploys monitoring devices:
   - strategically to collect organization-determined essential information;
   - at ad hoc locations to track specific types of transactions of interest to the state;
d. 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; and
e. Obtains legal opinion with regard to monitoring activities in accordance with applicable federal laws, Executive Orders, directives, policies, or regulations.

The State of Montana employs automated tools to support near real-time analysis of events.

The State of Montana monitors inbound and outbound communications for unusual or unauthorized activities or conditions. The State of Montana provides near real-time alerts when the following indications of compromise or potential compromise occur: account privilege escalation, authentication, antivirus/antimalware software, user changes, log errors, system failures, and other network anomalies.

The State of Montana prevents non-privileged users from circumventing intrusion detection and prevention capabilities.

Control Number	Control Name	Priority	Control Baseline
SI-5	Security Alerts, Advisories, and Directives	P1	SI-5

The State of Montana:
a. Receives security alerts, advisories, and directives from designated external organizations on an ongoing basis;
b. Generates internal security alerts, advisories, and directives as deemed necessary;
c. Disseminates security alerts, advisories, and directives to appropriate entity/agency security contacts for their use and distribution; and
d. Implements security directives in accordance with established time frames, or notifies the issuing organization of the degree of noncompliance.

Control Number	Control Name	Priority	Control Baseline
SI-7	Software, Firmware, and Information Integrity	P1	SI-7 (1) (7)

The State of Montana 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.

The State of Montana incorporates the detection of unauthorized changes to software into the organizational incident response capability.

Control Number	Control Name	Priority	Control Baseline
SI-8	Spam Protection	P1	SI-8 (1) (2)

The State of Montana:

a. Employs spam protection mechanisms at entry and exit points and at workstations, servers, or mobile computing devices on the network to detect and take action on unsolicited messages transported by electronic mail, electronic mail attachments, web accesses, or other common means; and
b. Updates spam protection mechanisms (including signature definitions) daily, or when new releases are available.

The State of Montana centrally manages spam protection mechanisms.

Control Number	Control Name	Priority	Control Baseline
SI-10	Information Input Validation	P1	SI-10

The State of Montana Information systems check the validity of information inputs.

Control Number	Control Name	Priority	Control Baseline
SI-11	Error Handling	P2	SI-11

The State of Montana Information systems:

a. Identify potentially security-relevant error conditions;
b. Generate error messages that provide information necessary for corrective actions without revealing sensitive, operational information vital to State business in error logs and administrative messages that could be exploited by adversaries; and
c. Reveal sensitive error messages only to authorized personnel.

Control Number	Control Name	Priority	Control Baseline
SI-12	Information Handling and Retention	P2	SI-12

The State of Montana handles and retains both information within and output from information systems in accordance with applicable laws, Executive Orders, directives, policies, regulations, standards, and operational requirements.

Control Number	Control Name	Priority	Control Baseline
SI-16	Memory Protection	P0	SI-16

The State of Montana information systems implement security safeguards to protect its memory from unauthorized code execution.

FAMILY/Category: Program Management (PM)

Control Number	Control Name	Priority	Control Baseline
PM-1	Information Security Program Plan	P1	PM-1

The State of Montana:

a. Develops and disseminates an organization-wide information security program plan that:
   - Provides an overview of the requirements for the security program and a description of the security program management controls and common controls in place or planned for meeting those requirements;
   - Provides sufficient information about the program management controls and common controls to enable an implementation that is unambiguously compliant with the intent of the plan and a determination of the risk to be incurred if the plan is implemented as intended;
   - Includes roles, responsibilities, management commitment, coordination among organizational entities, and compliance;
   - Is approved by a senior official with responsibility and accountability for the risk being incurred to organizational operations, organizational assets, individuals, other organizations, and the State;

b. Reviews State-wide information security program plan every two years; and

c. Revises the plan to address organizational changes and problems identified during plan implementation or security control assessments.

Control Number	Control Name	Priority	Control Baseline
PM-2	Senior Information Security Officer	P1	PM-2
The State of Montana appoints a senior information security officer with the mission and resources to coordinate, develop, implement, and maintain a State-wide information security program.			

The State of Montana appoints a senior information security officer with the mission and resources to coordinate, develop, implement, and maintain a State-wide information security program.

Control Number	Control Name	Priority	Control Baseline
PM-3	Information Security Resources	P1	PM-3

The State of Montana:

a. Ensures that all capital planning and investment requests include the resources needed to implement the information security program and documents all exceptions to this requirement;

b. Employs a business case to record the resources required; and

c. Ensures that information security resources are available for expenditure as planned.

Control Number	Control Name	Priority	Control Baseline
PM-4	Plan of Action and Milestones Process	P1	PM-4

The State of Montana implements a process for ensuring that plans of action and milestones for the security program and the associated organizational information systems are:

a. Developed and maintained;

b. Document the remedial information security actions to mitigate risk to organizational operations and assets, individuals, other organizations, and the State; and

c. Are reported in accordance with State of Montana (OMB FISMA) reporting requirements.

Control Number	Control Name	Priority	Control Baseline
PM-5	Information System Inventory	P1	PM-5

The State of Montana develops and maintains an inventory of its information systems.

Control Number	Control Name	Priority	Control Baseline
PM-6	Information Security Measures of Performance	P1	PM-6

The State of Montana develops, monitors, and reports on the results of information security measures of performance.

Control Number	Control Name	Priority	Control Baseline
PM-7	Enterprise Architecture	P1	PM-7

The State of Montana develops enterprise architecture with consideration for information security and the resulting risk to organizational operations, organizational assets, individuals, other organizations, and the State.

Control Number	Control Name	Priority	Control Baseline
PM-8	Critical Infrastructure Plan	P1	PM-8

The State of Montana addresses information security issues in the development, documentation, and updating of a critical infrastructure and key resources protection plan.

Control Number	Control Name	Priority	Control Baseline
PM-9	Risk Management Strategy	P1	PM-9

The State of Montana:

a. Develops a comprehensive strategy to manage risk to organizational operations and assets, individuals, other organizations, and the State associated with the operation and use of information systems; and
b. Implements that strategy consistently across the state.

Control Number	Control Name	Priority	Control Baseline
PM-10	Security Authorization Process	P1	PM-10

The State of Montana:

a. Manages (i.e., documents, tracks, and reports) the security state of organizational information systems through security authorization processes;
b. Designates individuals to fulfill specific roles and responsibilities within the state risk management process; and
c. Fully integrates the security authorization processes into an organization-wide risk management program.

Control Number	Control Name	Priority	Control Baseline
PM-11	Mission/Business Process Definition	P1	PM-11

The State of Montana:

a. Defines mission/business processes with consideration for information security and the resulting risk to organizational operations, organizational assets, individuals, other organizations, and the State; and
b. Determines information protection needs arising from the defined mission/business processes and revises the processes as necessary, until an achievable set of protection needs is obtained.

Control Number	Control Name	Priority	Control Baseline
PM-12	Insider Threat Program	P1	PM-12

This control is a requirement of national classified information. The Executive branch of the State of Montana does not handle classified information. The state recommends that agencies with unclassified sensitive information should consider implementing an insider threat program that includes a cross-discipline insider threat incident handling team.

Control Number	Control Name	Priority	Control Baseline
PM-13	Information Security Workforce	P1	PM-13

The State of Montana establishes an information security workforce development and improvement program.

Control Number	Control Name	Priority	Control Baseline
PM-14	Testing, Training, and Monitoring	P1	PM-14

The State of Montana:

a. Implements a process for ensuring that organizational plans for conducting security testing, training, and monitoring activities associated with organizational information systems:

- Are developed and maintained; and
- Continue to be executed in a timely manner;

b. Reviews testing, training, and monitoring plans for consistency with the organizational risk management strategy and organization-wide priorities for risk response actions.

Control Number	Control Name	Priority	Control Baseline
PM-15	Contacts with Security Groups and Associations	P3	PM-15

The State of Montana establishes and institutionalizes contact with selected groups and associations within the security community:

a. To facilitate ongoing security education and training for organizational personnel;
b. To maintain currency with recommended security practices, techniques, and technologies; and
c. To share current security-related information including threats, vulnerabilities, and incidents.

Control Number	Control Name	Priority	Control Baseline
PM-16	Threat Awareness Program	P1	PM-16

The State of Montana implements a threat awareness program that includes a cross-organization information-sharing capability.

Definitions

Refer to the GDE-Statewide Glossary: Information Systems Policies and Standards for a list of local definitions.

Refer to the National Institute of Standards and Technology (NIST) Glossary of Key Information Security Terms for a list of NIST definitions.

References

Refer to the National Institute of Standards and Technology (NIST) Special Publication 800-53 Revision 4 APPENDIX D – Security Control Baselines Summary