

STATE OF MONTANA

Montana Information Security Advisory Council
Best Practices Workgroup – Media Protection Standards

Media Protection Standards



STATE OF MONTANA

Montana Information Security Advisory Council
Best Practices Workgroup – Media Protection Standards

1. Purpose

To further increase the overall security posture of the State of Montana, several agencies agreed to collaborate on a strategic goal of increasing security through efforts associated with media protection. The category of Media Protection as defined by NIST includes media access, media marking, media storage, media transport, and media sanitization. Because media protection often includes the identification of protective measures for data in-transit and at-rest, this summary also includes guidance on approved methods of encryption for the protection and security of sensitive information.

This document has been concurred upon by the MT-ISAC membership, and approved as an enterprise standard by the Chief Information Officer for the State of Montana.

2. Policy

Media Protection applies to the following controls found within the Information Security Policy.

a. [Information Security Policy](#)

- Identify
 - 1.1, 1.6, 1.7, 1.10
- Protect
 - 2.4, 2.9, 2.13, 2.15, 2.18, 2.19, 2.20
- Detect
- Respond
- Recover

b. [Information Security Policy – Appendix A](#)

- Access Control (AC)
 - AC-6 – Least Privilege
 - AC-19 – Access Control for Mobile Devices
 - AC-20 - Use of External Information Systems
- Configuration Management (CM)
 - CM-2 – Baseline Configuration
 - CM-5 – Access Restrictions for Change
 - CM-7 – Least Functionality
 - CM-8 - Information System Component Inventory
- Identification and Authentication (IA)
 - IA-2 – Identification and Authentication
 - IA-4 - Identifier Management
 - IA-7 – Cryptographic Module Authentication

STATE OF MONTANA

Montana Information Security Advisory Council
Best Practices Workgroup – Media Protection Standards

- Media Protection (MP), pages 17- 20
 - MP-1 – Media Protection Policy and Procedures
 - MP-2 – Media Access
 - MP-3 – Media Marking
 - MP-4 – Media Storage
 - MP-5 – Media Transport
 - MP-6 – Media Sanitization
 - MP-7 – Media Use
- Physical and Environmental Protection (PE)
 - PE-2 – Physical Access Authorizations
 - PE-3 – Physical Access Control
 - PE-4 - Access Control for Transmission Medium
 - PE-5 - Access Control for Output Devices
 - PE-6 - Monitoring Physical Access
 - PE-8 - Visitor Access Records
- Personnel Security (PS)
 - PS-3 – Personnel Screening
 - PS-6 – Access Agreements
 - PS-7 – Third-Party Personnel Security
- System and Communication Protection (SC)
 - SC-4 – Information in Shared Resources
 - SC-8 - Transmission Confidentiality and Integrity
 - SC-12 - Cryptographic Key Establishment and Management
 - SC-13 - Cryptographic Protection
- System and Information Integrity (SI)
 - SI-2 – Flaw Remediation (Patch Management)
 - SI-3 – Malicious Code Protection
 - SI-4 – Information System Monitoring
 - SI-7 – Software, Firmware, and Information Integrity
 - SI-16 – Memory Protection

Encryption applies to the following controls found within the Information Security Policy.

a. [Information Security Policy](#)

- Identify
 - 1.6, 1.7, 1.10
- Protect
 - 2.1, 2.5, 2.9, 2.13, 2.18

STATE OF MONTANA

Montana Information Security Advisory Council
Best Practices Workgroup – Media Protection Standards

- Detect
- Respond
- Recover

b. [Information Security Policy – Appendix A](#)

- Access Control (AC)
 - AC-17 – Remote Access
 - AC-18 – Wireless Access
- Identification and Authentication (IA)
 - IA-5 – Authenticator Management
 - IA-7 – Cryptographic Module Authentication
- Media Protection (MP)
 - MP-4 – Media Storage
 - MP-5 – Media Transport
- System and Communication Protection (SC)
 - SC-7 – Boundary Protection

3. Definitions of Media Types

“Digital media” includes memory devices in laptops and computers and any removable, transportable digital memory media. Examples may include: internal and external hard-drives in workstations, servers, printers, copiers, portable storage devices (USBs), laptops, tablets, CD’s, DVD’s, audio recorders, memory, etc.

“Non-digital” media includes paper and microfilm.

4. Media Protection Best-Practices (MP-2 through MP-7)

- Media Access
 - a) Implement [Hardening of Devices](#) standard
 - b) Follow the least privilege and role based rules for allowing access.
 - c) Restrict 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)
 - d) Permit only authorized access to Level 2 or Level 3 classified digital and Level 2 or Level 3 classified non-digital media classified per State of Montana’s [Data Classification](#) policy. See Attachment A for an abbreviated summary of classification levels.
 - e) Use of multifactor authentication when appropriate
 - f) Protect unmarked media until determining classification type

STATE OF MONTANA

Montana Information Security Advisory Council Best Practices Workgroup – Media Protection Standards

- g) Do not utilize publicly accessible computers to access, process, store, or transmit sensitive information. Publicly accessible computers include but are not limited to: hotel business center computers, convention center computers, public library computers, public kiosk computers, etc.
- h) Disable Autorun functionality of all computer systems (configuration management)
- i) Configure anti-malware/antivirus software to scan all removable media devices on insertion into computer systems
- o Media Marking
 - a) All state employees will identify removable electronic media and information system output in accordance with organizational policies and procedures for classification, handling caveats, and distribution limitations
 - b) Personnel shall label and identify paper and other output products containing Level 2 or Level 3 data
 - Stamps
 - Water marks
 - etc.
 - c) Identified staff are responsible for marking device(s)
- o Media Storage
 - a) All electronic media used for the storage of business-related materials must follow the purchasing criteria and requirements of the agency.
 - b) All portable devices containing Level 2 or Level 3 data shall be encrypted.
 - c) Only agency approved media device storage devices shall be permitted to be used with State IT resources.
 - d) Non-digital media classified at Level 2 or Level 3 must be secured in locked file cabinets or other locking storage areas (e.g. work area, desk drawers).
 - e) When information of mixed classification levels is stored at same location or on the same device, the highest storage level must be used.
 - f) Refer to Attachment A and B for specific at-rest protection techniques per data and hardware types.
- o Media Transport

Controls shall be in place to protect digital and non-digital media containing sensitive information while in transport (physically moved from one location to another) to prevent inadvertent or inappropriate disclosure and use.

 - a) For hard copy printouts that are mailed or shipped, agency must document procedures and only release to authorized individuals. Packages containing sensitive material are to be sent by method(s) that provide for complete shipment tracking and history, and signature confirmation of delivery.

STATE OF MONTANA

Montana Information Security Advisory Council Best Practices Workgroup – Media Protection Standards

- b) When information of mixed classification levels is transported/transferred to the same location or on the same device, the most restrictive technique must be used.
- c) Refer to Attachments A and B for specific in-transit protection techniques per data and hardware types.
- o Media Sanitization
 - a) All electronic storage devices must be sanitized following the State of Montana [Disposal of Media Storage Device](#) standard
 - Agencies must use vendors that are under contract with the State of Montana for media destruction, or following the purchasing process to procure a vendor to complete this task.
 - b) Paper documents must be locked up prior to shredding in locked waste bins if it contains sensitive information. These bins should not allow for retrieving materials within the bin.
 - Agencies must use vendors that are under contract with the State of Montana for media destruction, or following the purchasing process to procure a vendor to complete this task.
 - The threshold for shredding documents (e.g. cross-cut) should meet IRS Pub 1075 criteria to make the information unreadable and unusable.

A sample 1-page media protection guideline summary (Attachment C) is included that agencies can use, customize if necessary if their internal controls are more restrictive, and distribute to staff.

5. Compliance

Compliance shall be evidenced by the implementation of the NIST Media Protection standards and the related best practices as described above.

6. Conclusion

The Media Protection Standard Summary document is the result of a multi-agency collaboration and has the MT-ISAC Best Practices Work Group approval. The representatives from these groups worked to endorse the recommendations contained here-in. A methodical, well-planned approach to effectively testing and measuring these controls will introduce additional layers to the security of the State of Montana's end-users.

ATTACHMENT A

Media Protection Standards Per Information Type

* List includes all commonly used data types.

Summary of classification levels:

- **State of Montana Level 1** – Information available to the general public and eligible for public access. Data that is classified as State of Montana Level 1 would reside in *information systems* that are categorized as Low.
- **State of Montana Level 2** – Information that disclosure to third parties or the public is governed by specific laws (e.g. HIPAA, Criminal Justice Information, Federal Tax Information, etc.) that determine and protect confidentiality. Data that is classified as State of Montana Level 2 would reside in *information systems* that are categorized as medium.
- **State of Montana Level 3** – Information that, if divulged, could compromise or endanger citizens, employees, or safety assets of the State. Data that is classified as State of Montana Level 3 would reside in *information systems* that are categorized as high.

Data Type	In Transit Requirement	Protection Technique/Tool	At Rest Requirement	Required Protection Technique/Tool
Level 1	None	Verify Recipient	File Protection	AD-GPO, ACL
Level 2	Encryption	PKI email, SFTP, OneDrive	File Protection	PKE applications/devices, ACL, AD-GPO
Level 3	Encryption	PKI email, SFTP, OneDrive	File Protection	PKE applications/devices, ACL, AD-GPO
Enterprise Network/Data Flow Diagrams (State of MT agency related)	Encryption	PKI email, SFTP, OneDrive	File Protection	PKE applications/devices, ACL, AD-GPO
Federal Tax Information sent to IRS	File Compression & Encryption	WinZip or SecureZip (send the password via phone call)	File Protection	PKE applications/devices, ACL, AD-GPO, IRS Pub 1075
Drug Enforcement Agency (DEA) Number	Encryption	PKI email, SFTP, OneDrive	File Protection	PKE applications/devices, ACL, AD-GPO

Information Security Testing Results (State of MT agency related)	Encryption	PKI email, SFTP, OneDrive	File Protection	PKE applications/devices, ACL, AD-GPO
Information System Risk Assessments (State of MT agency related)	Encryption	PKI email, SFTP, OneDrive	File Protection	PKE applications/devices, ACL, AD-GPO
Information System Security Plans (State of MT agency related)	Encryption	PKI email, SFTP, OneDrive	File Protection	PKE applications/devices, ACL, AD-GPO
Mosaic information classified as Personal Information.	Encryption	PKI email, SFTP, OneDrive	File Protection	PKE applications/devices, ACL, AD-GPO
Examples:	SSN+First Name/Initial(FNI)+Last Name(LN)	DL/State ID/Tribal ID + FNI+LN	Acct#/CC#/Debit Card# + Password, Security code, or Access code for financial acct number + FNI + LN	
	Medical Information + FNI + LN	Taxpayer ID Number + FNI + LN	Identity Protection Personal ID# issued by IRS + FNI + LN	
Passwords (State of MT business related)	Encryption	PKI email, SFTP, OneDrive	Encryption	PKI used with EFS, Password Manager
Personally Identifiable Information (e.g. social security number, tax ID number, passport number, driver's license number)	Encryption	PKI email, SFTP, OneDrive	File Protection	PKE applications/devices, ACL, AD-GPO
Personal Financial Information (e.g. bank account numbers, credit card numbers, tax payer ID number)	Encryption	PKI email, SFTP, OneDrive	File Protection	PKE applications/devices, ACL, AD-GPO
Personal Health Information	Encryption	PKI email, SFTP, OneDrive	File Protection	PKE applications/devices, ACL, AD-GPO
Private Key Infrastructure (PKI) information used for Encryption	Encryption	PKI email, SFTP, OneDrive	Encryption	PKI used with EFS
Shared Folders (State of MT business related)	depends on data level classification	Protect at level of Data Type	depends on data level classification	Protect at level of Data classification level
System Logs (State of MT agency related)	Encryption	PKI email, SFTP, OneDrive	File Protection	PKE applications/devices, ACL, AD-GPO
When the right to individual privacy exceeds the merits of public disclosure, includes personal records, medical records, and other records	Encryption	PKI email, SFTP, OneDrive	File Protection	PKE applications/devices, ACL, AD-GPO
Wildlife Management Related: Name, Address, Phone #, DoB, SSN, and DL# when lawfully taking large predator	Encryption	PKI email, SFTP, OneDrive	File Protection	PKE applications/devices, ACL, AD-GPO

Active Directory (AD)
Group Policy Object (GPO)
Access Control List (ACL)
Public Key Enabled (PKE)
Public Key Infrastructure (PKI)
Microsoft Encrypted File System (EFS)

ATTACHMENT B

Media Protection Standards Per Hardware Type

Hardware Type	In Transit Requirement	Protection Technique/Tool	At Rest Requirement	Required Protection Technique/Tool
Laptop	Full Disk Encryption	BitLocker	Full Disk Encryption	BitLocker
Mobile Phone (fully managed/enrolled)	N/A	AirWatch	Encryption of all storage	MDM
SD Card	Full Disk Encryption	BitLocker	Full Disk Encryption	BitLocker
CD/DVD	Full Disk Encryption	BitLocker	Full Disk Encryption	BitLocker
Thumb Drive	Full Disk Encryption	BitLocker	Full Disk Encryption	BitLocker
External Hard Drive	Full Disk Encryption	BitLocker	Full Disk Encryption	BitLocker
Backup Disks/Tapes	Full Disk Encryption	BitLocker	Full Disk Encryption	BitLocker
DMZ Load Balancer	Encryption (internal)	Built into the system	File Protection	PKE applications/devices, ACL, AD-GPO
DMZ Load Balancer	Disconnect (external)	Physical	File Protection	PKE applications/devices, ACL, AD-GPO
Desktop	Physical Protection	Authorized Transport Method	File Protection	PKE applications/devices, ACL, AD-GPO
Server	Physical Protection	Authorized Transport Method	File Protection	PKE applications/devices, ACL, AD-GPO
Non-Digital Level 2/3 Couriered/Hand-Carried	Physical Protection	Authorized Transport Method	Physical Protection	Locked File Cabinet/Desk Drawer/Safe
Non-Digital Level 2/3 Shipped/Mailed	Physical Protection	Package Tracking + Signature Confirmation of Delivery	Physical Protection	Locked File Cabinet/Desk Drawer/Safe

ATTACHMENT C

SAMPLE Media Protection Guideline Summary

State of Montana Data Classification Levels	Media Protection Guideline				
	<i>Requirements are determined by the type of data and its risk</i>				
	Access	Storage	Markings	Transport	Sanitization
Level 1 <i>General public information</i> Risk category: Low	Public	No Limits	No Limits	No Limits	See Disposal of Media Storage Device Standard for details.
Level 2 Restricted/Sensitive <i>Information that disclosure to third parties or public is governed by specific law that determines and protect confidentially</i> Risk category: Moderate	Restricted Authorized personnel only	<ul style="list-style-type: none"> • In controlled access facility • In a controlled access area • In locked, labeled file cabinet or encrypted (digital media) 	<ul style="list-style-type: none"> • Restricted Distribution marked, Confidential, For Official Use Only 	<ul style="list-style-type: none"> • On encrypted agency owned storage device • Must be authorized to by Administrator to be transported outside controlled area • Hard copy documents must be secured in a locked container 	See Disposal of Media Storage Device Standard for details.
Level 3 RISTRICTED <i>Information that, if divulged, could compromise or endanger citizens, employees, or safety assets of the State</i> Risk category: High	Restricted Written authorization by Department Head	<ul style="list-style-type: none"> • In controlled access facility • In a controlled access area • In locked file cabinet • Secured at all times until sanitized or destroyed 	<ul style="list-style-type: none"> • Restricted Distribution marked Confidential, For Official Use Only 	<ul style="list-style-type: none"> • Written authorization by Department Head • On agency owned encrypted storage device and secured at all times • Hard copy documents secured in a locked briefcase or container outside controlled area 	See Disposal of Media Storage Device Standard for details.